ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M
MESTRADO
ENGENHARIA INFORMÁTICA

O SDLC e a proteção de Dados desde a Conceção e por Defeito

Michele Siqueira Braga Freitas

2018/2020

O SDLC e a proteção de Dados desde a Conceção e por Defeito
Michele Siqueira Braga Freitas

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M
MESTRADO
ENGENHARIA INFORMÁTICA

Michele Braga Freitas. O SDLC e a proteção de Dados desde a Conceção e por Defeito

2018/2020

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

M

MESTRADO
ENGENHARIA INFORMÁTICA

O SDLC e a proteção de Dados desde a Conceção e por Defeito

Michele Siqueira Braga Freitas

João Paulo Magalhães

Agradecimentos

A realização deste projeto de mestrado foi um caminho bem longo, mas graças a Deus foi possível superá-lo. Agradeço a Ele em primeiro lugar por chegar até aqui, também ao meu esposo Alcimar Freitas que sempre pude contar com apoio e incentivo, que mesmo com os obstáculos no caminho, nunca me deixou desistir. Agradeço imensamente ao meu orientador, Professor Doutor João Paulo Magalhães, pela grande orientação no trabalho, disponibilidade, por me acompanhar nesse caminho e pela revisão do documento. A empresa acolhedora no estágio/projeto GTI, ao meu tutor Filipe Pimentel e aos colegas de profissão por ajudar no inquérito do SDLC RGPD. Aos meus familiares e amigos do Brasil pela compreensão da ausência nesses dois anos, também pela torcida e orações. Ao meu filho Noah que está a caminho e que no meio desse trabalho surgiu para me dar mais força e vontade de finalizá-lo. Enfim, obrigada a todos que de alguma forma direta ou indiretamente contribuíram para realizar esse sonho e atingir o objetivo.

Resumo

Com a plena aplicabilidade do Regulamento Geral de Proteção de Dados (RGPD) na UE em 25 de maio 2018, a proteção de dados por *design* e por padrão se tornam obrigação legal aplicável. O Regulamento Geral de Proteção de Dados (RGPD) obriga as organizações a uma adaptação sobre a forma como tratam e protegem os dados pessoais e sensíveis. O consentimento explícito para recolha e tratamento de dados, reportar problemas relacionados com a segurança dos dados pessoais e a designação de um responsável pelo tratamento de dados (DPO) passou a ser obrigatório e já está a ser cumprido. Porém, questões como segurança por defeito e por padrão, numa perspetiva prática, estão ainda a dar os primeiros passos.

Neste projeto o objetivo é a criação de um processo e meios técnicos para dotar o software a desenvolver dos requisitos essenciais para obtenção da privacidade nos dados pessoais. Utilizando a metodologia de segurança para assim, obter maior conformidade com o RGPD alinhado com o SDLC e resultar em um processo para auxiliar os programadores durante o desenvolvimento das aplicações informáticas visando à segurança das informações pessoais.

Palavras-chave: RGPD, DPO, dados pessoais, segurança por defeito, segurança por padrão, SDLC.

Abstract

With the full application of the General Data Protection Regulation (GDPR) in the EU on 25 May 2018, data protection by design and by default become an applicable legal obligation. The General Data Protection Regulation (GDPR) obliges organizations to adapt how they handle and protect personal and sensitive data. Explicit consent for data collection and processing, reporting problems related to the security of personal data and the appointment of a data controller (DPO) has become mandatory and is already being complied with. However, issues like security by default and by default, from a practical perspective, are still taking their first steps.

In this project the objective is to create a process and technical means to provide the software to develop from essential requirements for obtaining privacy in personal data. Using the security methodology to achieve greater compliance with the GDPR in line with the SDLC and result in a process to assist programmers during the development of technical applications for the security of personal information.

Keywords: GDPR, DPO, personal data, security by default, security by default, SDLC.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÓNIMOS

AIDP - Avaliação de Impacto sobre a Proteção dos Dados

CCPA - California Consumer Privacy Act

CNPD - Comissão Nacional de Proteção de Dados

DPO – Data Protection Officer

EU – União Europeia

FIPs - Federal Information Processing Standards

HIPAA - Health Insurance Portability and Accountability Act

IEC - International Electrotechnical Commission

ISO – International Organization for Standardization

PII – Personally Identifiable Information

RGPD – Regulamento Geral de Proteção de Dados

SDLC – Software Development Life Cycle

SGBD - Sistema de Gerenciamento de Banco de Dados

TIC - Tecnologias da informação e comunicação

GLOSSÁRIO

Anonimização - Constitui um tratamento posterior de dados pessoais. Para anonimizar quaisquer dados, têm de lhes ser retirados elementos suficientes para que deixe de ser possível identificar o titular dos dados.

Aplicação - É um produto de software desenvolvido para suportar a realização das tarefas individuais das pessoas e a execução dos processos das organizações.

CNPD - Comissão Nacional de Proteção de Dados é uma entidade administrativa independente com poderes de autoridade que assegura o papel controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito. Ela é a responsável por aplicar coimas ao abrigo do RGPD às empresas que não cumprem o regulamento.

Controlador - Entidade, pessoa, agência ou autoridade pública responsável por determinar os propósitos e forma de processar os dados pessoais. No contexto deste documento assume-se que o controlador faz parte da mesma organização que o processador.

Controlo de Acesso - Meio que visa limitar o acesso às informações e ao processamento das mesmas impedindo assim o acesso a qualquer utilizador, funcionário ou terceiro que não tenha autorização para tal. Em caso de autorização de acesso, os mesmos são responsabilizados pelos seus atos e também pela proteção das suas informações de autenticação.

CRUD - Create, Read, Update e Delete, são as quatro operações básicas (criação, consulta, atualização e apagamento de dados) utilizadas em bases de dados relacionais fornecidas aos utilizadores do sistema.

Dados Pessoais - Qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (”titular dos dados”); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um identificador como o nome, número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, económica, cultural ou social.

Encarregado de Proteção de Dados - Data Protection Officer (DPO) no seu termo original, traduzindo para português o Encarregado de Proteção de Dados, uma pessoa nomeada pelo controlador e o processador para apoiar nas atividades base do RGPD e garantir que a organização está em conformidade com o regulamento.

Fugas de informação - Uma falha na segurança que pode levar ao comprometimento dos princípios da segurança, nomeadamente à destruição, perda, alteração, divulgação e/ou acesso não autorizados de dados pessoais.

Indivíduos / Titulares dos dados - Pessoas que podem ser identificadas direta ou indiretamente, sobre quem os dados pessoais são tratados.

Minimização - A minimização de dados é dos princípios de proteção de dados que indica que só devem ser recolhidos e tratados os dados essências para o fim a que se destinam.

Mockup - Modelo ou uma representação em escala ou de tamanho real de um projeto. É utilizado para apresentar uma ideia de forma elaborada com design muito próximo ao final do produto.

Ofuscação - É o processo de ocultar ou esconder dados de identificação pessoal de forma elevar o grau de proteção das informações pessoais.

PME - Pequenas e médias empresas, são empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros (Europeia, 2006). São divididas em três tipos: micro, pequena e média empresa, que é definida de acordo com o número de colaboradores e o volume de negócios anual.

Processador - Entidade, pessoa, agência ou autoridade pública que processa os dados em nome do controlador. No contexto deste documento assume-se que o processador faz parte da mesma organização que o controlador.

Pseudonimização - É uma forma de processar dados pessoais, aplicando filtros que garantam a partir de um conjunto ou conjuntos de dados não ser possível identificar, por parte de pessoas não autorizadas, o titular dos mesmos.

RGPD - O Regulamento Geral de Proteção de Dados em si que é constituído por diversos artigos e definições necessários para a implementação e conformidade do mesmo.

Smoke Tests - O teste de aceitação é um teste preliminar para revelar falhas simples, graves o suficiente para, por exemplo, rejeitar uma versão em potencial do software.

TIC - Tecnologia da informação e comunicação (TIC) pode ser definida como um conjunto de recursos tecnológicos. Essa expressão se refere ao papel da comunicação (seja por fios, cabos, ou sem fio) na moderna tecnologia da informação. É utilizado em diversas formas como, na indústria (no processo de

automação), no comércio (no gerenciamento, nas diversas formas de publicidade), no setor de investimentos (informação simultânea, comunicação imediata) e na educação (no processo de ensino aprendizagem, na educação a distância).

Tratamento de Dados Pessoais - Qualquer operação ou conjunto de operações efetuados sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, comparação ou interconexão, bem como a limitação, apagamento ou destruição.

Violação de Dados Pessoais - Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Capítulo 1

Introdução

A privacidade dos dados pessoais é um assunto de extrema importância no cenário atual e tem vindo preocupar cada vez mais os cidadãos, principalmente após as revelações de Snowden em 2013, que expôs a NSA dizendo que esta espiava centenas de milhões de pessoas e que poderia elaborar um perfil detalhado de grande parte delas. De forma regular observam-se notícias de grandes empresas que foram ou são alvos de ataques por parte de *hackers* que procuram na maioria das vezes comprometer os dados do negócio e obter um valor monetário através da venda. Nesses casos são dados que na grande maioria das vezes contém dados pessoais e cuja o seu comprometimento causa impacto negativo na vida das pessoas. Um exemplo foi a fuga de informações no caso do Ashley Madison. Temos ainda as coimas elevadas que as organizações são obrigadas a pagar e a perda da reputação que dificilmente é recuperada [1].

A criação de um regulamento que especifica as medidas, desde recolha, processamento, armazenamento e transmissão de dados pessoais para que as empresas tomem medidas adequadas à sua proteção foi colocado em prática e levou a uma adaptação por parte das empresas. O objetivo envolve a criação de aplicações informáticas mais seguras, meios para evitar que os dados pessoais sejam obtidos por entidades cujo propósito seja tratar os dados de forma diferente pelo qual os dados foram recolhidos inicialmente ou entidades maliciosas. Aos titulares dos dados são dadas maiores garantias como o direito à informação sobre a forma como são tratados os seus dados pessoais.

Com a plena aplicabilidade do Regulamento Geral de Proteção de Dados na UE em 25 de maio 2018 [2], a proteção de dados por *design* e por padrão se torna uma obrigação legal aplicável. As organizações devem adaptar o modo como elas fazem o tratamento e cuidam dos dados pessoais e sensíveis. O RGPD preconiza a gestão da privacidade dos cidadãos e das suas informações pessoais. Além disso o RGPD traz novos direitos, como é o caso da portabilidade dos dados através do qual um indivíduo pode solicitar a transferência dos seus dados entre prestadores de serviços/entidades ou o seu esquecimento no qual uma pessoa pode pedir para, por exemplo, não receber mais informação ou ser contatado por um prestador de serviços.

O mesmo regulamento veio exigir às organizações a nomeação de um responsável pelo tratamento de dados. De acordo com o descrito em [3], o responsável pelo tratamento dos dados pessoais, designado por Data Protection Officer (DPO), deve aplicar medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica

do tratamento. O consentimento explícito para usar e tratar os dados pessoais do cidadão é obrigatório, bem como fica sendo obrigatório que as organizações tenham de informar qualquer problema que haja com relação à segurança desses dados. Compete também ao DPO, estabelecer a correta Política de Proteção de Dados em toda e organização.

O RGPD prevê coimas elevadas caso ocorra violação dos dados pessoais e, nalguns casos, sanções criminais que, segundo o apresentado em [4], podem ser classificadas como de menor e maior gravidade. A de menor gravidade pode atingir coimas até 10 milhões de euros ou 2% do volume mundial de negócios do grupo onde a empresa se insere. As coimas para casos de maior gravidade podem ascender a 20 milhões de euros ou 4% do volume de negócios mundial.

Em 2019, segundo o relatório apresentado em [5], as principais violações de dados causaram 402,6 milhões de euros de multas as organizações que não protegeram corretamente as informações do consumidor. É de referir também que as três maiores coimas atingiram grande parte do valor sendo de quase 365 milhões de euros. A primeira da lista das empresas afetadas é a British Airways que foi multada por 204,6 milhões de euros. Esta foi a maior coima registada no mundo por usar clonagem de cartão para coletar informações pessoais e de pagamento dos seus clientes. A segunda maior coima de acordo com essa mesma fonte foi de 110,3 milhões de euros, devido a um acidente cibernético ocorrido pela multinacional americana Marriott International, que causou a exposição de 339 milhões de registos de hóspedes. Em terceiro lugar, com uma multa de 50 milhões de euros, foi a empresa Google com violações ocorridas em 2019. A Figura 1.1 ilustra as empresas que sofreram as penalidades com as violações dos dados.

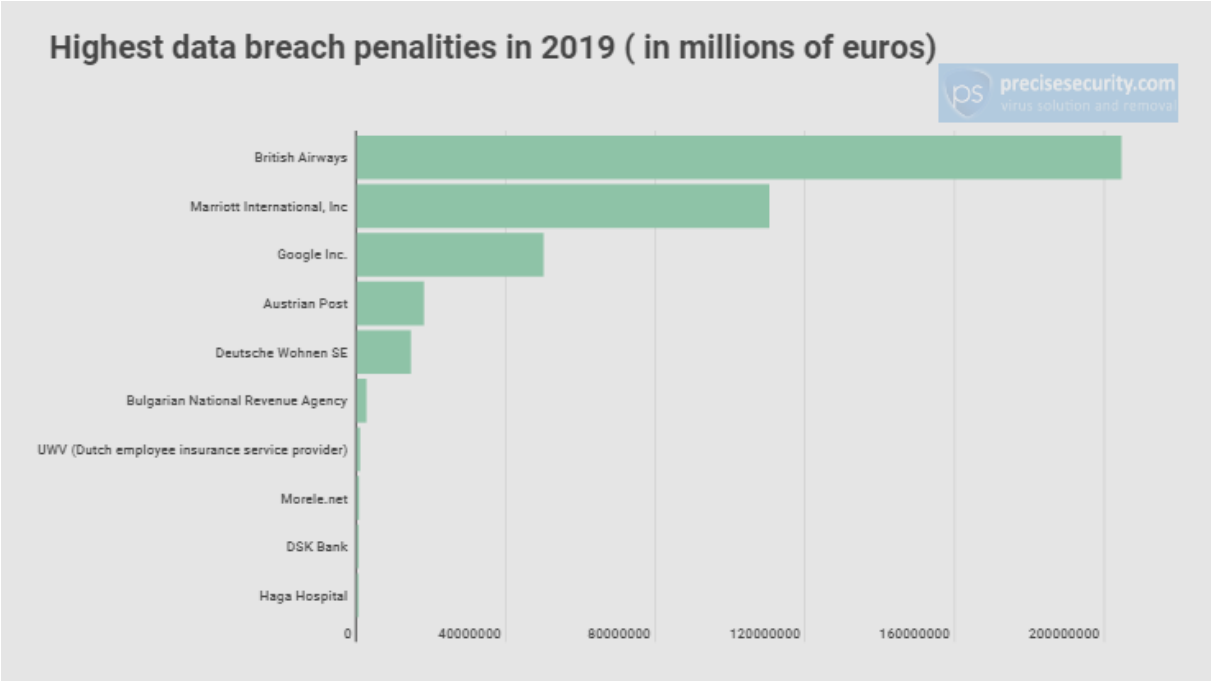


Figura 1.1 - Principais violações do RGPD em 2019 [5]

Os fatos apresentados enfatizam o quão importante são as organizações investirem em soluções para aumentar a segurança dos dados pessoais dos seus clientes, caso contrário pode sofrer coimas avultadas além da perda de reputação e quebra de confiança dos clientes.

1.1 Apresentação e Oportunidade do Tema

Este projeto visa criar um processo e meios técnicos para dotar o software a desenvolver dos requisitos essenciais para obtenção da privacidade nos dados pessoais. De acordo com [6], os dados a recolher e a armazenar devem ser adequados, relevantes e limitados ao estritamente necessário para o propósito do seu processamento. A segurança dos mesmos deverá ser aplicada de base e por defeito devendo para tal ser adotados princípios que os torne o seu processamento o mais seguro possível, protegendo os seus titulares e as organizações que recolhem e processam os dados pessoais.

Para a criação do processo de referência serão utilizadas normas (e.g.: ISO 27018, 29100, 29134, 29151) enquadráveis com os princípios do RGPD. O resultado será um processo ligado ao ciclo de desenvolvimento de software (SDLC) com os princípios e meios (controlos) que facultem o desenvolvimento de aplicações informáticas confiáveis e seguras desde a conceção e por defeito de acordo com os artigos 5º e 25º do RGPD [7]. A segurança por *design* [8] é uma abordagem que garante questões de privacidade e proteção de dados desde a fase de *design* de qualquer sistema. E a segurança por padrão, de acordo com [8], exige o processamento apenas dos dados necessários para atingir seu objetivo específico, de acordo com os padrões *Fair Information Practices* (FIPs) documentada em [9],

que contempla a especificação de finalidade, limitação de coleta, minimização de dados e limitação de uso.

O processo a desenvolver será elaborado a partir do *input* de intervenientes nas áreas chave, nomeadamente DPO e equipas de desenvolvimento. O mesmo será ainda aplicado na empresa GTI, local onde decorre um estágio associado a este projeto. É de referir, no entanto que o processo a criar é transversal podendo ser aplicado a qualquer organização que faça desenvolvimento de aplicações informáticas.

1.2 Objetivos principais

O objetivo deste trabalho é criar um processo alinhado com as várias fases do ciclo de desenvolvimento de software auxiliando a adoção dos princípios definidos pelo RGPD no software (por defeito desde a conceção). Para alcançar tal objetivo é necessário percorrer um caminho, que envolve a análise de referências na área da segurança da informação, proteção de dados e na definição de um processo que faça o alinhamento entre tarefas e ações para cada uma das fases do SDLC. Por exemplo, considerando a fase de desenho do SDLC, o procedimento deverá contemplar questões como minimização de dados, pseudonimização, anonimização e cifra. Deste modo, na fase de implementação estas questões serão tidas em consideração e os formulários dos aplicativos irão considerar apenas os dados estritamente necessários, e serão definidas vistas sobre os dados consoante o perfil do utilizador e tirado partido de mecanismos de ofuscação e cifra que muitos do SGBD atuais disponibilizam.

Espera-se que com a definição de tal processo, o desenvolvimento do software passe a integrar desde a conceção e por defeito controlos que maximizem o nível de conformidade com o RGPD. Desta forma as organizações estarão a cumprir o regulamento e, por isso, mais seguras dos seus procedimentos e protegidas contra eventuais situações de perda de dados e penalizações que decorrem dessa perda.

As equipas envolvidas no SDLC ficarão também mais suportadas com a definição clara de tarefas e ações a executar em cada uma das fases, com maior conhecimento sobre as exigências do RGPD, da sua importância no alinhamento entre ambos e do impacto positivo dessa prática adotada para a organização no nível de segurança dos seus produtos e serviços.

1.3 Contributos inovadores

Este trabalho contempla um conjunto de contributos para a área da segurança da informação, proteção de dados pessoais e desenvolvimento de software. A saber prevê:

1. Processo para o desenvolvimento de software contemplando segurança por padrão desde a conceção.
2. Criação de softwares alinhados com os princípios do RGPD e por isso mais seguros relativamente à proteção de dados pessoais.
3. Maior nível de conformidade das organizações com o RGPD, pelo uso de um processo simples e alinhado com o SDLC facilitando a sua aplicação pelos vários intervenientes.

1.4 Estrutura do documento

Esta dissertação é composta por 6 capítulos. No capítulo 2 é apresentado o estado da arte. A metodologia subjacente ao desenvolvimento do trabalho é apresentada no capítulo 3. No quarto capítulo é apresentado um inquérito para aferir a interligação atual entre o RGPD e o ciclo de desenvolvimento de software e respetiva análise de resultados. O capítulo 5 apresenta um conjunto de procedimentos que, por cada fase do SDLC, acrescenta a visão do RGPD. Por último, no capítulo 6 é feita a conclusão do trabalho.

Capítulo 2

Estado da Arte

A proteção dos dados e a privacidade é uma preocupação em todo o mundo. O contínuo aumento da atividade *online* faz com que essa questão ganhe ainda mais destaque. Para fazer face à preocupação tem sido adotada legislação e regulamentos que visam melhorar a proteção de dados pessoais, adequando os direitos e deveres quer dos titulares dos dados como dos que processam esses dados. De acordo com [10], dos 194 países existentes no mundo, 132 adotaram uma legislação para garantir a proteção e privacidade dos dados. A Figura 2.1 ilustra o mapa mundo relativamente ao estado da legislação para a proteção de dados pessoais.

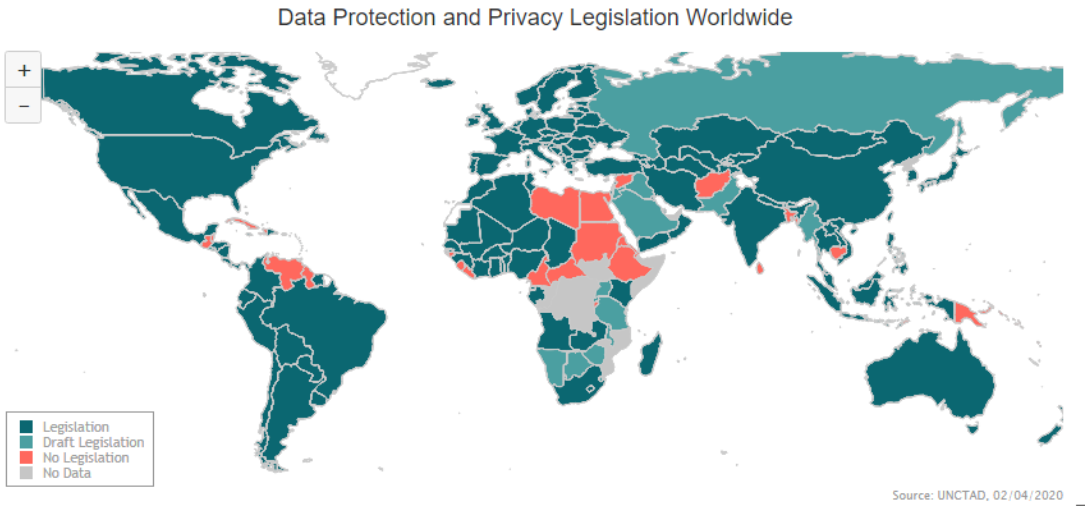


Figura 2.1 - Estado da legislação para proteção de dados e privacidade no mundo [10]

Essa fonte [10] mostra que no mundo todo 66% dos países possuem legislação, 10% têm projeto de lei, 19% não possuem legislação e 5% sem dados. Portugal, tal como ilustrado na Figura 2.2, é um dos países que adota legislação de proteção ao consumidor, privacidade e proteção de dados e legislação para crimes cibernéticos.

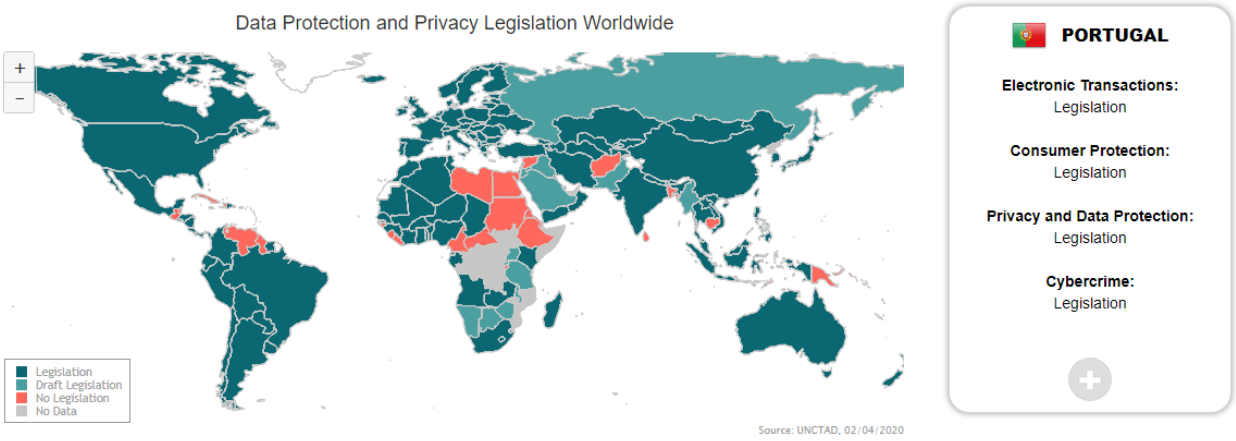


Figura 2.2 - Proteção de dados e legislação em Portugal [10]

Além do RGPD que é o regulamento da Europa, há diversos tipos de regulamentos com leis de privacidade e muitos projetos de lei no mundo. De acordo com [11] houve um aumento dessas leis de 120 para 132 em 2019. O aumento de 10% são jurisdições que possuem leis de privacidade de dados que abrangem tanto o setor público quanto o privado. Dentre os doze países com novas leis estão:

- Ilhas Cayman (Caribe) - Lei de Proteção de Dados 2017, Lei 33 de 2017.
- Mauritânia (África Ocidental) - Lei 2017-020 sobre a proteção de dados pessoais.
- Níger (África Ocidental) – Lei 2017-28 relativo à proteção de dados de pessoais
- Guiné-Conakry - República da Guiné (África Ocidental) - Lei / 2016/037 / AN relativa à cibersegurança e proteção de dados pessoais
- Argélia (Norte da África) - Lei nº 18-07 datado de 10 de junho de 2018 sobre a proteção no processamento de dados com autorização prévia.
- Panamá (América do Sul) - A Lei de Proteção de Dados Pessoais.
- St Kitts & Nevis (Caribe) - A Lei de Proteção de Dados e a lei complementar de Liberdade de Informação.
- Líbano (Oriente Médio) - A Lei de Transações Eletrônicas e Dados Pessoais.
- Bahrein (Oriente Médio) - A Lei do Bahrein sobre a Proteção de Dados Pessoais.
- Butão (Sul da Ásia) - A Lei de Informação, Comunicação e Mídia do Butão, mínima de privacidade de dados, que se aplica apenas ao fornecimento dos Setores de TIC e Mídia.
- República Popular da China (Norte da Ásia) - A Lei de Segurança Cibernética e a Lei do Comércio Eletrônico de 2018 (em vigor em 1º de janeiro de 2019).
- Brasil (América do Sul) - Lei Geral de Privacidade de Dados (LGPD) do Brasil (Lei nº13.709 de 14 de agosto de 2018), lei de privacidade de dados que se baseia substancialmente no RGPD da Europa, com requisitos semelhantes avaliações de impacto de proteção de dados, oficiais de proteção de dados, notificações de violação ao titular dos dados e multas administrativas de até 2% da receita de uma empresa no ano anterior no Brasil.

Ainda, e segundo [11], das 132 leis pode-se comparar o número de países com leis de privacidade de dados e o resultado percentual como apresentado na Tabela 2.1.

Region	Countries	DP Laws	%
Africa	58	25	43%
Caribbean	29	12	41%
Other European	29	26	90%
EU	28	28	100%
Asia	28	15	54%
Latin America	22	12	55%
Middle East	14	8	57%
Pacific Islands	13	0	0%
Central Asia	6	2	33%
N. America	2	2	100%
Australasia	2	2	100%
TOTAL	231	132	57%

Tabela 2.1 - Lista de países e percentual dos que possuem lei de privacidade dos dados

Ainda que haja uma tendência para alargar o âmbito de aplicação da legislação, existe exemplos de regulamentos mais específicos. O California Consumer Privacy Act (CCPA) ou Lei de Proteção de Dados da Califórnia e o Health Insurance Portability and Accountability Act (HIPAA) ou Lei de Portabilidade e Responsabilidade dos Planos de Saúde, são leis aprovadas pelo estado da Califórnia e leis federais dos EUA que visam a privacidade regulando os dados focando quase que exclusivamente segundo [12], na portabilidade de dados de saúde e simplificação administrativa. Outro foco do HIPAA é a privacidade e segurança com relação aos dados de saúde, como por exemplo um hospital que usa os dados de saúde do paciente, a lei cobra diretamente do programa de seguro de saúde. Em [12] é dito que essas leis têm lacunas relacionados à privacidade, como registos eletrônicos de saúde e portabilidade pelo que houve apelos para a reformulação da lei, pois não atende todos os cenários que deveria. Ocorrem conflitos entre o CCPA e o HIPAA à medida que cada estado cria sua própria lei de privacidade de dados, sendo defendida como a solução a criação de uma lei federal de privacidade de dados.

Na Europa o Regulamento Geral de Proteção de Dados (RGPD) entrou em vigor a 25 de maio de 2018. Como apresentado em [13] o Regulamento (EU) 2016/679 do Parlamento Europeu é relativo à proteção das pessoas singulares, ao tratamento de dados pessoais e à livre circulação desses dados. Pretende ser um regulamento único para todos estados membros e é considerado um modelo de êxito para outros países.

O RGPD, de acordo com o descrito em [14], é aplicável a todas as organizações que oferecem produtos ou serviços na União Europeia ou monitorizam dados pessoais dos residentes, sendo aplicado mesmo se o processamento de dados pessoais ocorrer fora da Europa. Portanto, qualquer organização que lide com informações pessoais dos cidadãos da União Europeia deve obedecer ao RGPD. Organizações que não cumpram com o regulamento estão sujeitas a uma coima de valor considerável que é determinado, tal como apresentado na Tabela 2.2, de acordo com o montante máximo previsto e a percentagem do volume de negócio anual da organização.

Tipo empresa	Tipo de contraordenação			
	Muito grave		grave	
	Montante	% do volume de negócio anual	Montante	% do volume de negócio anual
Grande empresa	De € 5000 a € 20 000 000	4	De € 2500 a € 10 000 000	2
PME	De € 2000 a € 2 000 000	4	De € 1000 a € 1 000 000	2
Pessoas singulares	De € 1000 a € 500 000	-	De € 500 a € 250 000	-

Tabela 2.2 - Valores das coimas aplicadas pela CNPD [13]

Em [13] é referido um inquérito realizado em maio 2019 pelo RGPD. Através deste inquérito verificou-se que das 716 PME situadas na Espanha, Reino Unido, França e Irlanda, 50% não cumprem dois fatores crítico do regulamento que são a licitude e a transparência. Em Portugal, segundo o que é apresentado em [15], após a entrada em vigor do RGPD, foram abertos 610 processos de natureza contraordenacional, mantendo-se a tendência de aumento das denúncias ou mesmo de queixas dos cidadãos, que se totalizaram em 439. O claro aumento da demanda pode significar a atenção ao novo Regulamento demonstrado por outras autoridades, pois delas foram recebidas participações das quais emergiram 173 processos e foram iniciadas 7 averiguações por iniciativa da CNPD (Comissão Nacional de Proteção de Dados). Decorrente desta atividade, desde 25 de maio de 2018, a CNPD aplicou 22 coimas em Portugal, num valor total de 408 990,40 euros.

As organizações devem provar que mantém conformidade com o RGPD. A segurança dos dados deve ocorrer através de medidas técnicas e organizativas que garantam um nível de segurança adequado ao risco [4]. De acordo com o disposto no artigo 32º RGPD [16], essas medidas podem ser traduzidas por exemplo na pseudonimização e cifra dos dados pessoais. Assegurar a confidencialidade e integridade do tratamento, possuir os meios necessários para, em tempo razoável, recuperar o normal tratamento dos dados em caso de se verificar alguma avaria técnica, efetuar com prontidão testes de qualidade da segurança que devem ser documentados para garantir a segurança e proteção dos dados pessoais são também medidas de conformidade que devem ser tomadas e registadas para que facilmente sejam demonstradas às entidades reguladoras.

O artigo 5º do RGPD , define os dados pessoais, como sendo um objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (licitude, lealdade e transparência) [17]. Define que os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. De acordo com [3], o artigo 25º do

RGPD, a proteção de dados deve ser feita desde a conceção e por defeito, devendo as organizações aplicar com eficácia as medidas técnicas, tais como pseudonimização, garantindo os princípios de proteção dos dados e privacidade, como a minimização. De forma geral o RGPD reforça que a segurança da informação deve ser uma preocupação das organizações. Garantir a segurança e a conformidade, requer a avaliação, implementação e manutenção contínua. Porém, verificou-se à entrada em vigor do RGPD, uma preocupação das empresas em dar resposta formal ao que era exigido. Foi designado um responsável de dados e foram tornados os consentimentos explícitos. Já as questões como minimização, pseudonimização e cifra de dados foram deixadas para segundo plano. Estas questões são pertinentes e estritamente ligadas as aplicações informáticas (considerando a via digital de tratamento de dados) sendo por isso essencial que as empresas reformulem ou considerem a inclusão de controlos nas aplicações informáticas que tratem dados pessoais, ficando desta forma ainda mais alinhadas com os princípios do RGPD.

O Systems Development Life Cycle (SDLC) [18], ou Ciclo de Vida de Desenvolvimento de Sistemas, é utilizado para desenvolvimento, manutenção e substituição, que proporciona uma visão global dos aspetos associados na construção e utilização do software. Desde o início do processo de conceção é essencial e necessário os cuidados com a privacidade dos dados e com a segurança. O SDLC refere-se aos estágios de conceção, projeto, criação e implementação de um sistema de informação e os modelos e metodologias para a construção, visando a qualidade que atenda aos requisitos definidos e dentro do prazo e custos estipulados. Tal como referido, sendo o software uma ferramenta base na recolha e processamento de dados pessoais torna-se fundamental alinhar o seu desenvolvimento com o RGPD permitindo assim a conceção de software alinhado com os princípios do Regulamento Geral sobre a Proteção de Dados.

2.1 O Ciclo de Vida do Desenvolvimento de Software (SDLC) e o RGPD

O SDLC é dividido em seis fases, desde o levantamento de requisitos até a manutenção. A forma como as fases são executadas varia de empresa para empresa e muitas vezes de projeto para projeto. Com o RGPD surge a necessidade de criar softwares alinhados com os princípios da proteção de dados pessoais. Assim, e combinando o SDLC com o RGPD temos de um lado fases, e do outro, princípios a garantir sob a forma de controlos. Na literatura não se encontram ainda referências específicas que façam um alinhamento técnico entre ambos, levando-nos a focar a nossa análise nas fases e nos princípios para posterior combinação entre ambos.

As fases do SDLC são análise, desenho, implementação, teste, implantação, manutenção. De acordo com [19] elas consistem:

- **Análise de Requisitos:** Reunir os requisitos discutindo com o cliente as necessidades em relação ao desenvolvimento do software. Sendo o objetivo dessa fase, pegar todos os detalhes do projeto, capturando os detalhes de cada requisito e assim, garantir que todos entendam o projeto e como cada requisito será atendido. Segundo [20] os requisitos dos software expressam as necessidades e restrições a considerar durante o desenvolvimento**.**

- **Desenho ou *Design*:** Inicia o *design* de alto nível do software para atender a cada requisito da fase anterior. Detalhes técnicos são discutidos nessa fase e vários parâmetros, assim como os riscos, tecnologias a ser usado, restrições do projeto, tempo, entre outros.

- **Implementação:** Fase onde são implementados todos os requisitos. São divididos os trabalhos como criação de banco de dados e a codificação do software.

- **Teste:** Nessa fase é verificado se o software está funcionando de acordo com o esperado ou se precisa de alguma correção. Também é verificado se ele preenche os requisitos definidos no início do projeto. O teste de software [20] é uma parte obrigatória, para avaliar a qualidade do sistema e se proceder à sua melhoria por meio de identificação de falhas e dos potenciais problemas.

- **Implantação:** Após o desenvolvimento e os testes serem concluídos, nessa fase o software é implantado ou instalado para o cliente com as funcionalidades definidas.

- **Manutenção:** Depois de implantado o software, uma equipa geralmente fica responsável por cuidar de qualquer problema. Essa fase [20] lida com falhas, alterações tecnológicas e as evoluções dos requisitos dos utilizadores.

Segundo cláusula apresentada em [21], na especificação e análise de requisitos, devem ser incluído a segurança da informação. E quando existir alguma alteração na plataforma de produção, durante as revisões, convém que as aplicações críticas de negócio sejam analisadas e testadas, assegurando que não ocorra impacto nas operações organizacionais e na segurança da informação.

Os princípios do o RGPD são descritos em [21] e focam:

- **Licitude, lealdade e transparência**: "Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados" Art.5.1(a). O tratamento de dados pessoais, independentemente de quão pequeno seja, tem de assentar numa base legal sólida. Os responsáveis pelo tratamento de dados pessoais precisam fornecer uma visão bem clara sobre o funcionamento do tratamento dos dados e quais as consequências, antes de recolher e tratá-los.

- **Limitação das finalidades**: "Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º, nº 1" RGPD Art.5.1(b). Limitação de propósito requer que os responsáveis pelo tratamento de dados tenham definidas as razões de recolha e tratamento dos dados. Além de que, a investigação dos dados em todo o seu ciclo de vida é necessário para saber quando o tratamento deles não acontecer de acordo com a intuito inicial.

- **Minimização dos dados**: "Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados" RGPD Art.5.1(c). A minimização de dados envolve reduzir a quantidade de dados recolhidos ao estritamente necessário para que a interação com o titular dos dados seja satisfeita. Medidas técnicas: Armazenamento centralizado, ofuscação dos dados, remoção de meta-dados não utilizados e elementos intermediários.

- **Exatidão**: "Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora" RGPD Art.5.1(d). Exatidão consiste em tomar as medidas necessárias para garantir a precisão dos dados obtidos assim como, verificar a fonte dos mesmos.

- **Limitação da conservação**: Concentra-se em conservar os dados pessoais somente para o período em que os dados respondam as suas finalidades. Os responsáveis pelo tratamento de dados possuem total responsabilidade em manter o controlo deles e removê-los quando não estiverem sendo tratados de acordo com a sua finalidade original.

- **Segurança (Integridade e Confidencialidade)**: "Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando medidas técnicas ou organizativas adequadas" RGPD Art.5.1(f). Devem ser implementadas as medidas de segurança adequadas à proteção dos dados pessoais. Sendo que, a integridade e confidencialidade são conceitos fundamentais de segurança da informação, com isso protegendo a privacidade do titular dos dados, mantendo a sua integridade, exatidão e consistência dos dados armazenados. RGPD Art.5.2. Os responsáveis pelo tratamento de dados devem ser responsáveis e demonstrar conformidade com as disposições do regulamento. Medidas técnicas: autenticação e autorização, registos de auditoria à prova de violações, monitorização, mecanismos de prevenção de perda de dados (Data Loss Prevention).

Também com a introdução do RGPD, existe um conjunto de direitos dos titulares dos dados [21]. Entre os direitos temos:

- O **direito a ser informado**: Os titulares dos dados pessoais têm o direito a obter informações legíveis de que forma estão sendo tratados os seus dados.

- O **direito de acesso**: Os titulares dos dados podem fazer um pedido de acesso e obtenção de cópia de todos os seus dados pessoais que são processados.

- O **direito à remoção** (direito ao esquecimento): Os titulares dos dados possuem o direito de, em determinadas circunstâncias, pedir a remoção dos seus dados e podendo exigir aos responsáveis pelo tratamento deles que eliminem todos os dados a seu respeito.

- O **direito à portabilidade**: Os titulares dos dados têm o direito de solicitar uma cópia dos seus dados pessoais em formato de dados compreensível por máquinas e de transferi-los para qualquer outra empresa.

Além dos direitos o RGPD impõe também a concretização de:

- **Consentimento explícito:** De acordo com o novo regulamento, as empresas têm de pedir e receber o consentimento para a recolha, utilização e movimentação dos dados pessoais. Esta solicitação deve ser evidenciável, compreensível e de fácil acesso. O consentimento deve ser livre, informado, específico, expresso e claro.

- **Encarregados da Proteção dos Dados** (DPO): Ao abrigo do RGPD, os requisitos de manutenção de registos internos e a nomeação de um encarregado de proteção de dados para a organização são de carater obrigatórios.

- **Notificações obrigatórias** em caso de violação dos dados: No caso de existir uma violação dos dados (e.g. *data leak*), os responsáveis pelo seu tratamento devem notificar aos utilizadores e as autoridades. O prazo máximo é de 72 horas após descobrir que houve a violação.

De acordo com [22] existem dois tipos de sistemas para resolver o problema de *data leaks*. Um deles o sistema de deteção de vazamento (DLD – Data Leak Detection), que apesar de não fornecer proteção absoluta dos dados, é essencial para identificar vazamentos de dados o mais rápido possível. Um exemplo desse sistema é o serviço Hivecode Data Leak Detection [22], fornece o rastreio do banco de dados do utilizador, verificando com regularidade os emails propagados em banco de dados não autorizado, que se tornam suspeitos e assim notifica o usuário sobre o possível vazamento. O segundo sistema [22] seria o sistema de prevenção de perda de dados (DLP – Data Loss Prevention), que complementa o anterior com a funcionalidade adicional em realizar algumas ações nos dados encontrados, para assim, evitar futura divulgação deles. Um exemplo do DLP é o Google Cloud Data Loss Prevention, com funcionalidades de deteção de dados em uso dos seus 120 Infotypes (entidades que descrevem informações a serem detetadas) e outras ferramentas com objetivo de classificar, mascarar, tokenizar e transformar. No trabalho referenciado anteriormente, foi criado um outro tipo de sistema com objetivo de detetar *data leaks* em sites públicos com a funcionalidade do Apache Nutch [22] e detetar tipos críticos de dados.
Caso durante o ciclo do desenvolvimento do sistema, houver a preocupação de aplicar os princípios definidos em regulamentos como o RGPD, a segurança e privacidade do software sairá a ganhar com isso.

2.2 Software e a privacidade por defeito e por padrão

A privacidade dos dados no desenvolvimento de um software deve ser tratada desde a conceção. De acordo com [23] o objetivo da privacidade por *design* é atender aos requisitos de privacidade em todo processo de desenvolvimento do sistema, desde a conceção até sua disponibilização em produção. Para isso e como se retira de [24], deve-se fazer uma avaliação inicial cuidadosa e fazer a implementação de medidas e procedimentos técnicos, organizacionais desde do início, garantindo assim, o tratamento em conformidade com o RGPD, protegendo os direitos dos titulares de dados em questão. O trabalho apresentado em [25] mostra que questões relacionadas com a privacidade são fáceis de compreender, uma vez que é fácil entender o que significa a divulgação de informação pessoal, sensível ou confidencial de forma não autorizada, e qual o impacto que poderá ter para uma organização. O mesmo

trabalho diz que identificar e entender quais são os riscos existentes é o primeiro passo para a implementação do conceito *Privacy by Design*, pois só assim é possível implementar as medidas necessárias, também designados por controlos, para melhorar a privacidade. A falha em desenhar e implementar adequadamente uma aplicação, incapacidade de detetar um problema ou aplicar uma correção (*patch*) sem os testes adequados poderá resultar numa violação de privacidade.

Um SGSI (Sistema de Gestão de Segurança da Informação) [26] permite à empresa mitigar o risco de segurança atribuídos aos seus ativos, adequando a área de negócio. O objetivo é garantir a integridade e a disponibilidade da informação, sendo estes fatores necessários para que um sistema de uma organização seja considerado. As boas práticas para a criação de tais sistemas é patente na família das normas de segurança 27000 [27]. O benefício do SGSI é a redução de risco de responsabilidade por não precisar implementar ou determinar políticas e procedimentos, também diminuir o custo para a organização, aumentar a confiança com os parceiros e acima de tudo alinhamento com os requisitos legais.

A norma ISO/IEC 29100 fornece uma estrutura de alto nível para proteção de informações de identificação pessoal (PII) nos sistemas de tecnologia da informação e comunicação (TIC). As organizações que seguirem essa norma no ciclo de desenvolvimento do sistema, possuirão controlo de privacidade necessário e proteção relacionados às PII, pois terão a base para iniciar padronização de privacidade citadas em [25]. O *design* de qualquer sistema que envolva o processamento de PII deve ser precedido por uma identificação de requisitos relevantes à proteção da privacidade antes de serem implementados. E o gerenciamento de riscos descritos em [25] também são importantes para direcionar e controlar uma organização com relação ao risco de privacidade, melhorando o processo.

Os princípios de privacidade devem ser usados para orientar o *design*, desenvolvimento e implementação de políticas de privacidade e controlos. Estes princípios, de acordo com [25], são:

- **Consentimento e escolha**: Apresentar ao titular de PII a escolha para permitir ou não o processamento das suas informações;

- **Legitimidade e especificação do objetivo**: Garantir que o(s) objetivo(s) esteja conforme a lei aplicável e baseado em um suporte legal permitido;

- **Limitação de coleta**: Limitar a coleta de PII dentro dos limites que se aplicam a lei e sejam estritamente necessária para a finalidade especificada;

- **Minimização de dados**: A minimização de dados está intimamente ligada ao conceito de "limitação de coleta", minimiza a recolha e processamento de PII ao estritamente indispensável;

- **Limitação de uso, retenção e divulgação**: Reduzir a transferência de PII ao necessário, a fim de cumprir objetivos específicos, explícitos e legítimos; reter as PII apenas pelo tempo necessário para cumprir os propósitos declarados e posteriormente, destruir com segurança;

- **Precisão e qualidade**: Garantir que as PII processadas sejam precisas, completas e actualizadas;

- **Abertura, transparência e aviso**: Fornecer aos responsáveis pelas PII, informações claras e facilmente acessíveis sobre as políticas do controlador e finalidade para a qual estão sendo processadas;

- **Participação e acesso individuais**: Fornecer aos titulares das PII a capacidade de acessar e rever suas informações, permitir que os responsáveis pelas informações pessoais contestem a precisão e a integridade dos dados e as alterem no contexto específico;

- **Responsabilização**: Documentar e informar, conforme apropriado, todas as políticas, métodos e práticas com relação à privacidade;

- **Segurança da informação**: Proteger as PII sob sua autoridade com os controlos adequados aos níveis operacionais, funcionais e estratégico. Assim e de acordo com [21], aumentar o nível de maturidade relativamente a segurança das informações;

- **Conformidade com a privacidade**: Verificar e certificar que o processamento atenda à proteção de dados e à proteção da privacidade de requisitos através de auditorias periódicas.

As normas ISO [28], trazem conceitos que normalizam a segurança da informação em serviços prestados em nuvem. A ISO/IEC 27018 estabelece controlos e diretrizes referentes à implementação de medidas para a proteção da Informação de Identificação Pessoal (PII). O tratamento e utilização da PII são influenciadas por vários fatores, entre os quais o local onde os dados são armazenados, como por exemplo de acordo com [29] ambiente de serviço em nuvem, que é considerado um espaço de risco específico, que as organizações devem, através de requisitos considerados no *design* do sistema, garantir

a proteção das informações de identificação pessoal com medidas durante o desenvolvimento e implantação.

A norma ISO / IEC 29151: 2017 [30] estabelece objetivos e diretrizes para implementar controlos, para atender aos requisitos identificados por uma avaliação de risco e impacto relacionada à proteção da Informação de Identificação Pessoal (PII). A norma, tal como é dito em [31], aplica-se a todos os tipos e tamanhos de organizações que atuam com responsabilidades de controlador ou processador de dados pessoais.

Já a ISO / IEC 29134: 2017 é um documento voltado para a Avaliação de Impacto de Privacidade (PIA) das PII e inclui considerações, processos, sistemas ou programas de informação, onde é de acordo com o publicado em [32] relevante para os envolvidos na conceção ou implementação de projetos, incluindo as partes que operam sistemas e serviços de processamento de dados que processam PII. Ela inclui um método de análise de risco de fluxo de negócios e gerenciamento de riscos. Está alinhada com o processo de preparação, implementação e elaboração de relatórios. Faz parte da melhoria do sistema de implementação, identificar cobertura, critérios de avaliação e desenvolvimento de cronograma com engajamento das partes interessadas. O gerenciamento de riscos reflete-se no ciclo do desenvolvimento do software. A avaliação de impacto "reduz" ou "evita" o risco e deve ser realizada para o efeito.

2.3. Resumo do capítulo

Ao longo deste capítulo foram apresentados conceitos fundamentas relacionados com o desenvolvimento de software e a integração no mesmo de controlos que visam a segurança da informação pessoal. O alinhamento entre o ciclo de desenvolvimento de software e o mapeamento com os controlos refletidos na regulamentação, como é o caso do RGPD bem como o enquadramento geral de normas para a implementação de sistemas seguros foi apresentada. Nos próximos capítulos estes temas serão alvo de aprofundamento, sobretudo numa vertente prática de suporte à criação de um processo que alinha o SDLC e o RGPD.

Capítulo 3

Proposta do Trabalho

3.1 Metodologia de Investigação

A metodologia de investigação é instrumentalista e do tipo orientada ao problema. A sua dimensão é prescritiva na medida em que se pretende desenvolver um processo para ser aplicado em circunstâncias específicas como é o caso do desenvolvimento de software alinhado com o RGPD. O tipo de abordagem à investigação é orientado pela Engenharia [33].

A proposta de trabalho consiste na criação de um processo geral para auxiliar o as fases do desenvolvimento de software, desde conceção, ou seja, durante todo Ciclo de Vida de Desenvolvimento do Software. Tal como o resultado apresentado em [25], este trabalho pode ser visto como uma solução particular de uma metodologia de segurança, com o seu próprio conjunto de funcionalidades.

O processo será testado através de *use-case* que consistirá na aplicação do processo na empresa de acolhimento do estágio. A empresa já adota boas práticas de acordo com o RGPD implementadas pelo DPO. Com o novo processo em prática será possível adicionar na implementação de *software* o conceito de *Privacy by Design e Privacy by Default*, causando um grande impacto na organização, de forma a garantir privacidade dos dados pessoais aumentando ainda mais a segurança das informações e alinhamento com o RGPD.

O primeiro conceito considera questões de privacidade e proteção de dados na fase de *design* do sistema ao longo do ciclo de vida. O outro envolve proteção dos dados por padrão, fazendo com os dados a serem processados estejam vinculados aos princípios fundamentais de proteção de dados, como minimização, anonimização, cifra e pseudonimização.
Uma visão inicial, e de alto nível, do processo a desenvolver é apresentado na Tabela 3.1.

FASES SDLC	SDLC	RGPD	RGPD AÇÕES	PROCEDIMENTOS
ANÁLISE	Coleta das informações/ Especificação de requisitos funcionais e não funcionais	Especificação de requisitos de segurança de PII	Questionário/entrevista para determinar se a aplicação faz uso de dados pessoais e que tipo de dados pessoais	Doc de requisitos: SDLC-RGPD-01
DESENHO		Incluir no desenho do software	Especificar que perfis aplicacionais existentes, que	Consentimento; Minimização; Pseudonimização -

	Arquitetura de software	aspetos relacionados com o RGPD nomeadamente, minimização, gestão de acessos, proteção (anonimização, pseudonimização, cifra)	dados são necessários recolher por parte dos utilizadores, onde vão ser armazenados os dados, quem tem acesso e a que dados (matriz)	Doc desenho SDLC-RGPD-02
IMPLEMENTAÇÃO	O desenho do software é traduzido em código fonte	Codificação de acordo com os princípios do RGPD (identificados na fase de desenho)	Implementar o controlo de acessos considerando os perfis e o acesso a dados; considerar o local de armazenamento de dados com cifra forte	Gestão de acesso, anonimização, pseudonimização, cifra, Doc SDLC-RGPD-03
TESTE	Software desenvolvido é testado (testes funcionais e não funcionais)	Auditoria de segurança aplicacional com enfoque na PII	Auditoria à aplicação e base de dados; Consentimentos; Teste do controlo de acesso e da anonimização, pseudonimização, cifra tanto na aplicação como na BD e nos relatórios	Testes de segurança; Doc testes segurança SDLC-RGPD-04
IMPLANTAÇÃO	Disponibilizar a aplicação em produção	Conformidade dos fornecedores (APIs, Cloud, 3rd party);	Registo do processamento de dados pessoais e atividades dos usuários, mecanismos de esquecimento tanto em base de dados online como offline/backups, mecanismos de portabilidade	Registo de atividade e direitos exercidos pelos donos dos dados; Garantias dos fornecedores; Doc passagem a produção SDLC-RGPD-05
MANUTENÇÃO	Correção de algum problema ou aprimoramento detetado	Auditoria Contínua	Testes regulares à segurança aplicacional e PII e após atualizações, gestão de versões de aplicação e auditorias RGPD, Cópias de segurança	Cronograma e Registo de atividades programadas; Doc manutenção SDLC-RGPD-06

Tabela 3.1 - Visão inicial e alto nível do processo a desenvolver

Com a definição de um processo como o que é proposto, os dados a recolher e tratar serão especificados antes do início do processamento. Haverá boas práticas relativas à informação necessária a recolher e controlos que visem o processamento apenas dos dados necessários ao propósito da empresa. A capacidade para autenticar e autorizar todos os utilizadores e dispositivos, incluindo o controlo do acesso ao sistema e aplicações será documentado em conformidade com o RGPD e implementado com tais considerações. A ofuscação, pseudonimização e cifra farão parte do sistema aumentando a proteção dos dados pessoais.

Com um processo bem documentado e padronizado, as equipas de desenvolvimento de software ficam mais suportadas por documentos e boas práticas e em consequência a proteção e a privacidade das PII aumentará, atendendo ainda mais aos requisitos legais e regulamentares. A responsabilidade corporativa, a credibilidade do consumidor e o menor risco de violações de segurança saem também beneficiadas.

3.2 Inquérito de Avaliação no Desenvolvimento SDLC RGPD

No âmbito deste trabalho foi desenvolvido um inquérito com o objetivo de avaliar a interligação entre as fases do SDLC e o RGPD. O inquérito foi criado com programadores e DPO em mente.

A realização do inquérito é necessária para avaliar a importância que os profissionais e as empresas estão tendo em relação com a proteção dos dados pessoais e aferir se realizam uma avaliação de impacto com objetivo dessa proteção. O mesmo também permite analisar a adoção do RGPD durante o desenvolvimento de software e o nível de participação do DPO no projeto.

Além disso o inquérito permitirá perceber se nos últimos projetos desenvolvidos foram guardadas informações sobre data e hora do consentimento obtido e o canal utilizado. Se ocorreu a implementação de controlos de segurança de perfil para acesso às informações pessoais. As questões dos backup da aplicação e da base de dados são também assuntos em análise. Averiguar se há preocupações em manter a proteção de dados pessoais na fase de manutenção da aplicação faz parte do inquérito.

As respostas ao inquérito servem como guião ao desenho do processo, permitindo complementar e adaptar os formulários que acompanham cada procedimento associada a cada uma das fases do SDLC e que visa mapear aspetos do RGPD às fases.

Capítulo 4

Inquérito de Avaliação

O inquérito foi planeado para ser respondido por profissionais programadores e DPO, tendo sido disponibilizado durante uma semana. Foram enviados mais de quinhentos convites e mensagens pela rede social Linkedin, pedindo apenas três minutos do tempo dos participantes para colaborarem nas respostas ao inquérito do SDLC RGPD.

O percentual de respostas foi um pouco mais de 10% de todos os convites enviados, com isso, resultou em 54 respostas dos profissionais espalhados por diversas regiões de Portugal. Além do inquérito, foi criado um email de suporte para eventuais dúvidas sobre as perguntas do questionário.

O inquérito foi elaborado com 10 perguntas de resposta rápida em vários formatos para o profissional interagir e deixar sua opinião em relação ao assunto pertinente do trabalho sobre a proteção dos dados pessoais durante o desenvolvimento de *software* alinhado com o Regulamento Geral sobre a Proteção de Dados.

De acordo com as respostas obtidas na primeira pergunta como ilustrado na Figura 4.1, sobre a importância de realizar uma avaliação de impacto sobre a proteção dos dados (AIDP), 57,4 % que corresponde a maioria das respostas, acreditam ser muito importante fazê-la.

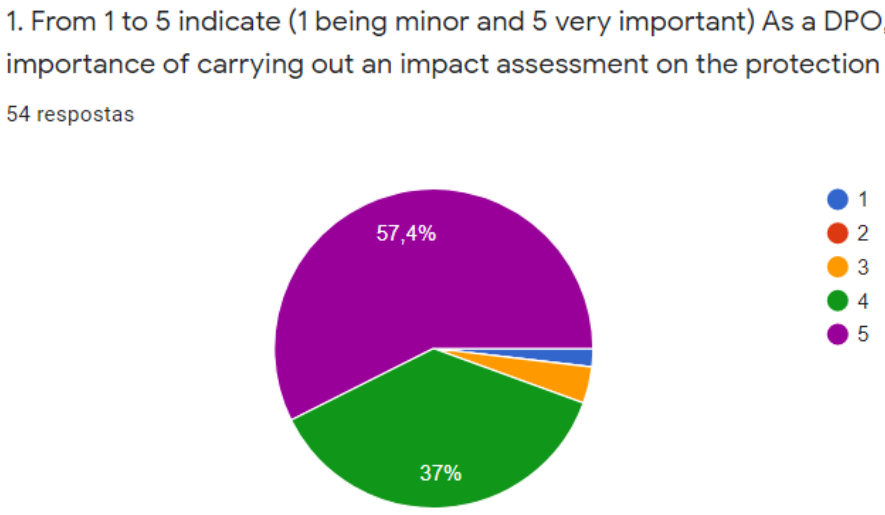


Figura 4.1 - Percentagem referente a primeira questão do inquérito AIPD

A questão dois questionou se a organização ou equipa adota algum processo para facilitar a adoção do RGPD durante o processo de desenvolvimento do software. A partir dessa informação, verificou-se que

a grande maioria com 66.7% fazem uso de algum tipo de processo não tendo sido especificado qual em concreto e 33.3% não utiliza nenhum processo durante o desenvolvimento de software. O resultado é ilustrado na Figura 4.2.

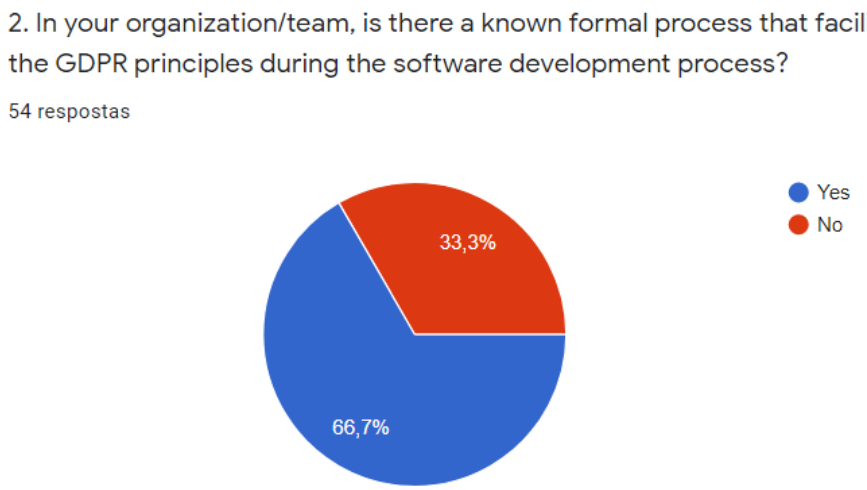


Figura 4.2 - Percentagens de pessoas que utilizaram algum processo durante o desenvolvimento

A questão seguinte, número três foi para verificar o papel do DPO e a equipa de desenvolvimento na criação de um novo projeto sobre os aspetos relacionados com o RGPD no *design* do aplicativo. De acordo com o resultado obtido, e ilustrado na Figura 4.3, 53,7% afirmam que ocorre uma discussão sobre o assunto na organização onde atuam, sendo que 24,1% disseram que não tem essa reunião e 22,2% não deram opinião sobre o assunto.

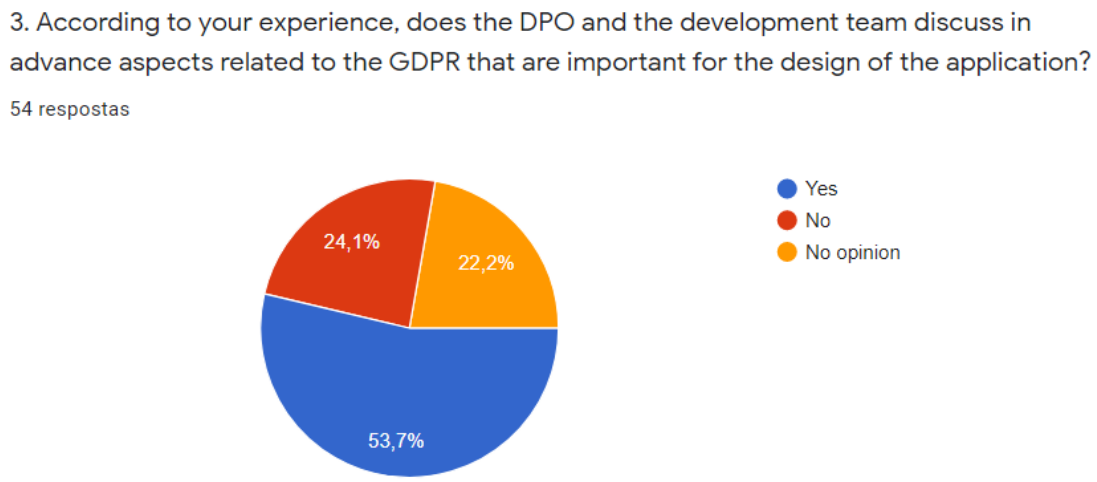


Figura 4.3 - Discussão do projeto entre DPO e equipa de Desenvolvimento sobre aspetos do RGPD

Na pergunta quatro, tal como ilustrado na Figura 4.4, foi abordado a opinião de 1 a 5, sendo 5 o grau maior de importância sobre existir um mapeamento de dados definindo o campo de dados, o usuário, a função e as ações CRUD antes de iniciar a implementação do nível de controlo de acesso a aplicação.

Todas que responderam consideram que existe alguma importância nessa prática, sendo que a maioria de 51,9% acredita ser muito importante ter uma ferramenta durante o processo do SDLC.

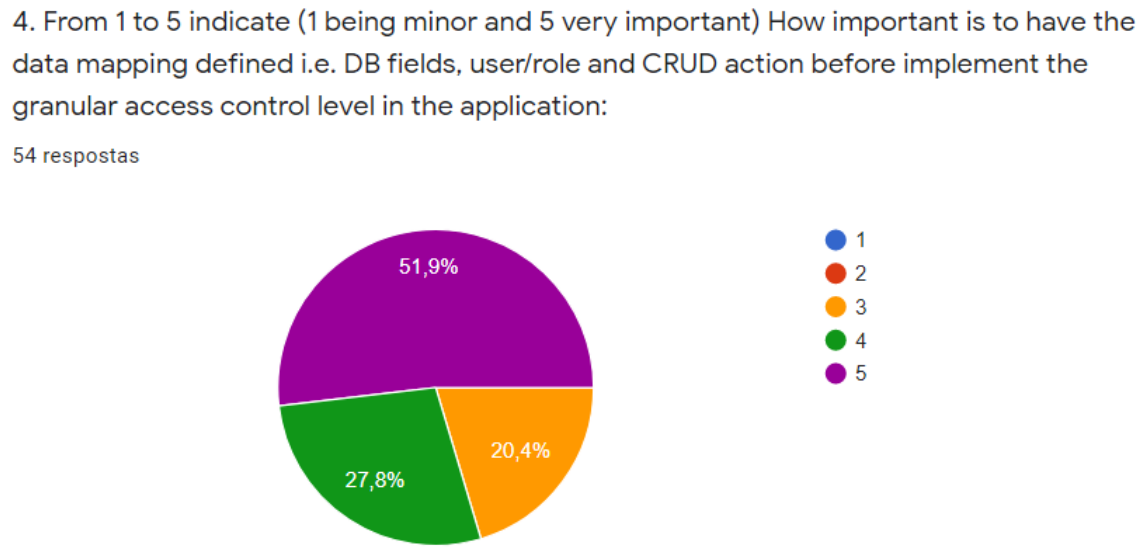


Figura 4.4 - Resultado sobre a importância de existir mapeamento de dados

O inquérito na questão cinco, focou-se o desenvolvimento de um aplicativo que se enquadra ao RGPD e contempla requisitos definidos no RGPD relativamente à forma de consentimento a adotar. A questão é acompanhada de considerações tal como apresentado na Tabela 4.1. As considerações são sobre a forma de consentimento e o que aborda cada uma delas, para averiguar quais foram utilizados pela equipa nos projetos finalizados anteriormente.

Free	Consent cannot be conditioned, that is, if the client does not give Consent, he does not have access to a certain product or service. The Data Owner may refuse or withdraw Consent without being harmed. Consent must be as easy to withdraw as it is to give.	<table><tr><td>Adopted</td><td>Not Adopted</td><td>Partially Adopted</td><td>Does not apply</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>
Informed	The Consent text must have a clear, simple, and easily accessible language. The Data Subject must be informed about the Purposes for which the Treatment is intended and about the right to withdraw Consent at any time.	<table><tr><td>Adopted</td><td>Not Adopted</td><td>Partially Adopted</td><td>Does not apply</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>
Specific	The data owner must be able to give a Consent for each Purpose of the Treatment (example: giving marketing authorization is different from giving marketing authorization to third parties).	<table><tr><td>Adopted</td><td>Not Adopted</td><td>Partially Adopted</td><td>Does not apply</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>
Express	The consent must be a positive act (written statement - including in electronic form - or	

	oral statement). Silence, pre-validated options, or omission do not constitute a Consent.	Adopted | Not Adopted | Partially Adopted | Does not apply | | | |	
Keep evidence	It should be possible to demonstrate that the Data Subject has given his / her Consent for the Treatment of his / her Personal Data, that is, it must be possible to register and prove the date / time when the Consent was obtained, the communication channel used and the version Consent.	Adopted | Not Adopted | Partially Adopted | Does not apply | | | |

Tabela 4.1 - Considerações sobre o consentimento de acordo com RGPD

A Figura 4.5. apresenta sobre a forma de gráfico de barras as respostas obtidas relativamente ao consentimento respeitar um conjunto de regras especificadas no RGPD. Como se verifica pelo gráfico o nível de adoção completo é sempre inferior a 50%.

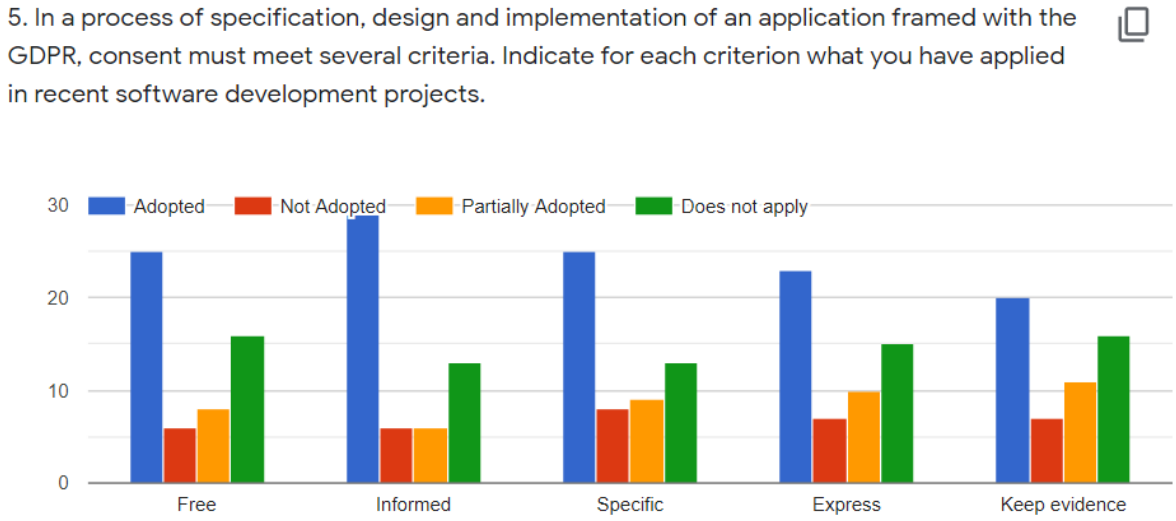


Figura 4.5 - Tipos de consentimento adotados nos projetos de desenvolvimento do software

Na questão seis, são apresentados exemplos de tipos de controlos de segurança adotados no desenvolvimento do software, tais como ofuscação, anonimização, pseudonimização e Encriptação, deixando campo para outro tipo de controlo. A questão aborda a adoção destes controlos e as respostas são ilustradas na Figura 4.6. Pode-se observar que a maioria dos desenvolvedores utilizaram em seus projetos a encriptação dos dados, correspondendo a 40 respostas com um percentual de 74,1% da pesquisa. Outros 25,9% usaram o controlo de anonimização dos dados e em terceiro lugar o controlo mais utilizado correspondeu ao de ofuscação dos dados com 22,2%. Das respostas recolhidas 11,1% disseram que não inseriram controlos nas suas aplicações e outros acrescentaram outros tipos de controlo utilizados.

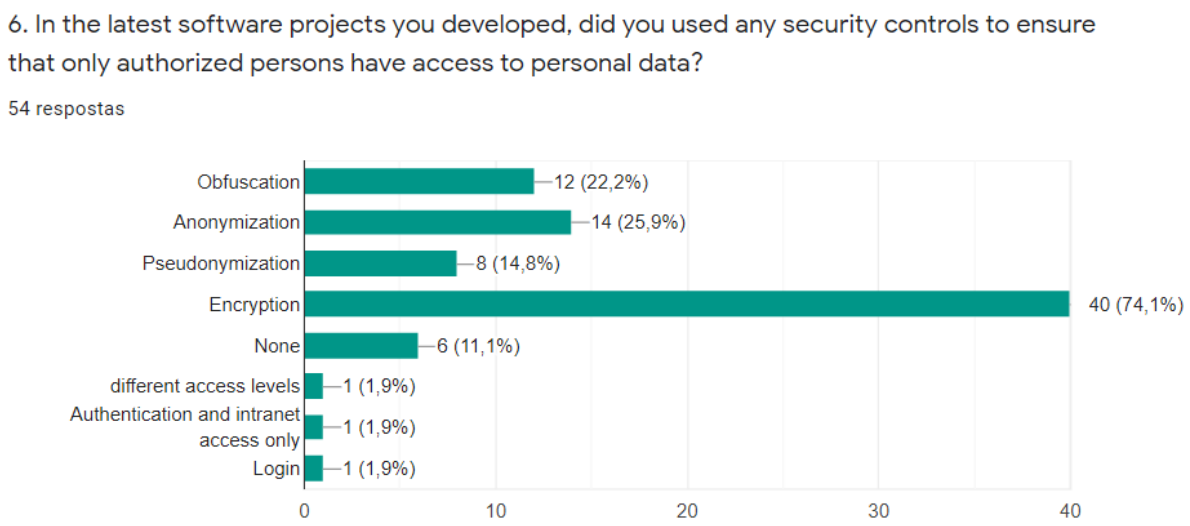


Figura 4.6 - Controlos utilizados nas aplicações pelos desenvolvedores

A questão sete interrogou os profissionais sobre quais direitos foram disponibilizados aos titulares dos dados. Com base na lista de direitos apresentados (direito de acesso, retificação, apagamento, portabilidade e esquecimento) os resultados obtidos são ilustrados na Figura 4.7. Como se verifica pelo resultado, a maioria dos programadores aplicaram nos seus projetos anteriores controlos de pedido de acesso aos dados, o pedido de retificação e o pedido de apagamento, sendo que a maioria não utilizou o direito de portabilidade nem esquecimento. Isto leva a concluir que as aplicações contemplam apenas o acesso ao perfil do utilizador, a atualização dos seus dados ou à eliminação do perfil.

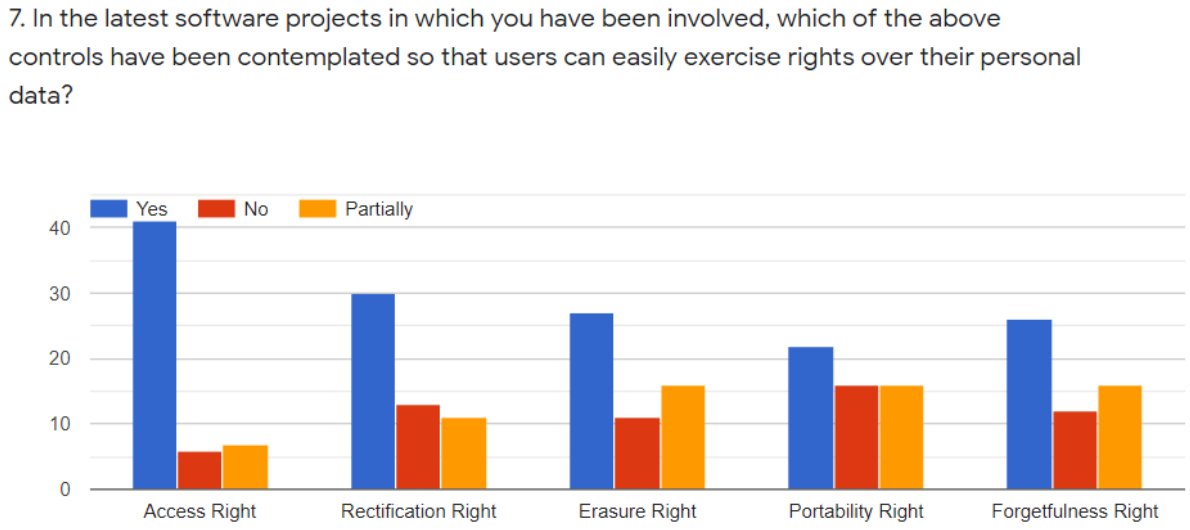


Figura 4.7 - Direitos dos utilizadores que foram utilizados nos projetos anteriores

Na pergunta número oito, questionou-se sobre o *backup* da aplicação e da base de dados, mais especificamente se o projeto desenvolvido teve consideração a salvaguarda e restauro alinhadas com o

RGPD. A maioria das respostas obtidas dos profissionais foi sim com 53,7%. Alguns não opinaram sobre o assunto 24,1% e outros 22,2% disseram que não, como apresentado abaixo na Figura 4.8.

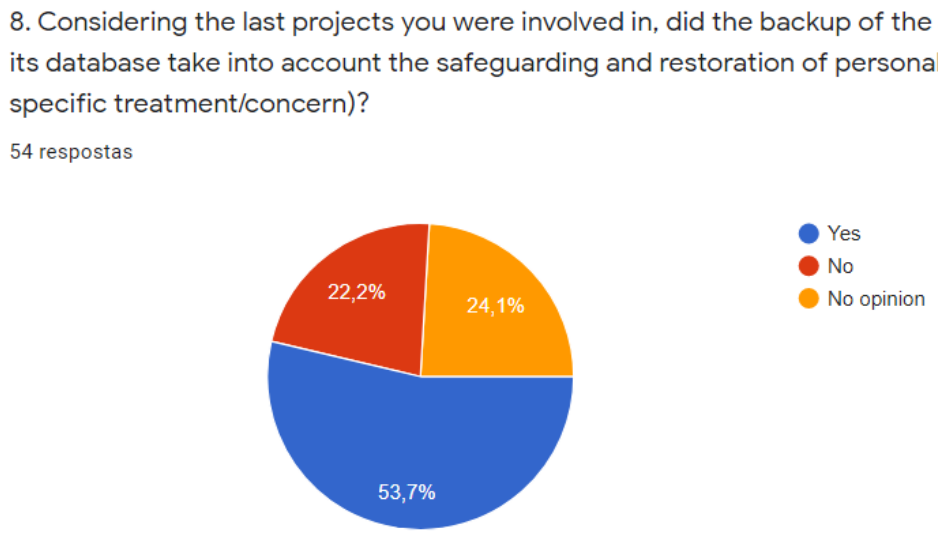


Figura 4.8 - Respostas sobre backup da aplicação e base de dados com o RGPD

A penúltima questão, indagou aos profissionais de tecnologia o quão útil eles consideram a existência de um processo para facilitar o desenho e a conceção de aplicações alinhadas ao RGPD. A maioria das pessoas investigadas responderam que consideram muito importante com um percentual de 38,9% do inquérito. 24,1% consideram apenas importante. Os resultados globais são ilustrados na Figura 4.9.

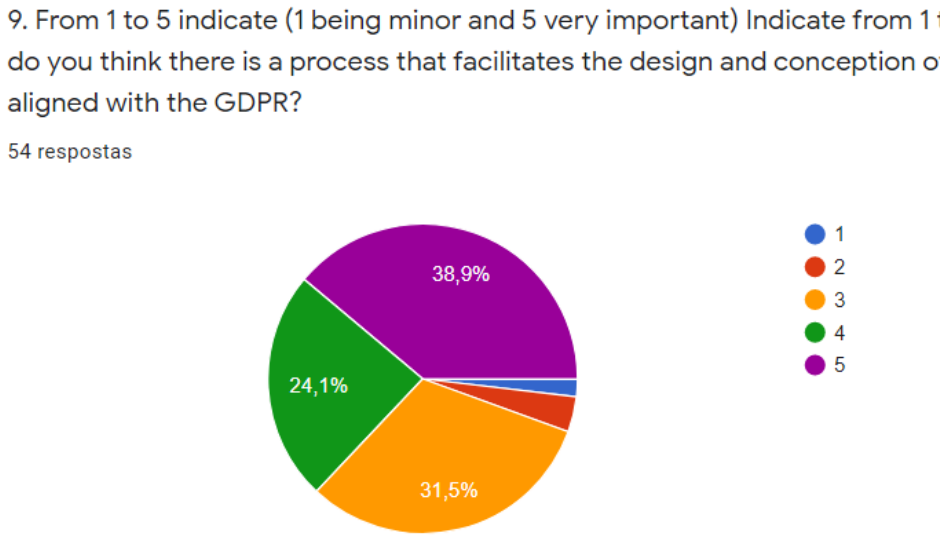


Figura 4.9 - Importância de um processo para facilitar desenho e conceção da aplicação

A última pergunta do inquérito, questionou-se, baseado na experiência dos profissionais se a equipa de segurança, o DPO e a equipa de desenvolvimento são sempre envolvidos na fase de manutenção do software e se existem nesta fase cuidados com a proteção dos dados. Com 46,3% das respostas os

profissionais afirmam que há sempre envolvimento. Outros 44,4% responderam que às vezes e 9,3% disseram que nunca. Estes resultados são apresentados na Figura 4.10.

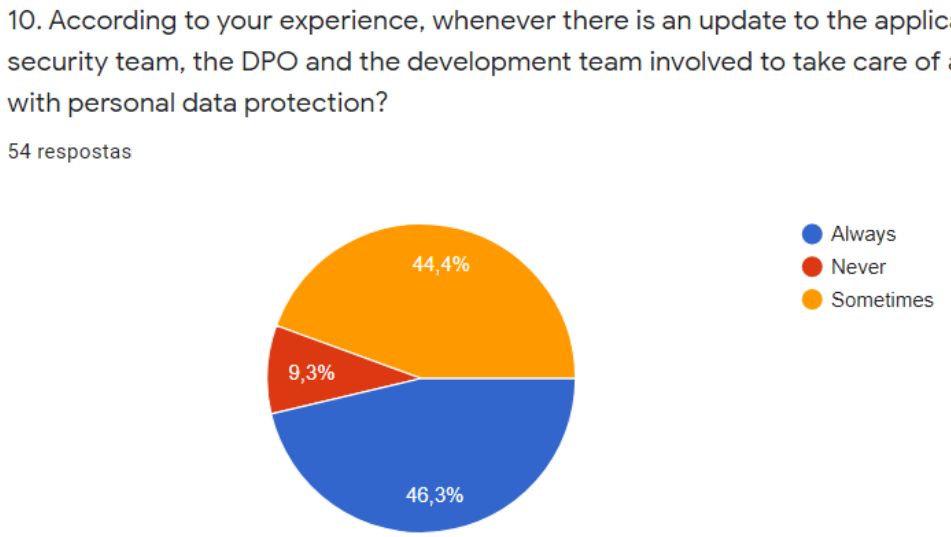


Figura 4.10 - Resultado das respostas sobre participação na atualização da aplicação

Através das respostas ao inquérito dirigido aos programadores e DPO de diversas organizações de tecnologia do país, foi possível verificar que a maioria tem conhecimento e dá importância ao Regulamento Geral sobre a Proteção de Dados, adotando medidas e controlos durante o desenvolvimento. Porém, também se verifica que muitos não possuem um processo para auxiliar durante o desenvolvimento das aplicações.

Existe um número muito grande de profissionais que não fazem avaliação de impacto sobre a proteção dos dados pessoais antes de iniciar um projeto, o que pode causar uma lacuna ou algum problema futuro no decorrer do desenvolvimento do software. Apesar de a maioria dos profissionais envolvidos na pesquisa terem a prática da discussão do projeto com o DPO e a equipa de desenvolvimento, ainda existe um número grande que não faz o envolvimento do DPO no projeto, potenciando falhas no alinhamento do SDLC com o RGPD nessas organizações.

O maior número das respostas aponta no sentido de ser muito importante haver um mapeamento de dados para ajudar no desenvolvimento, confirmando a importância desse trabalho para auxiliar os programadores durante a criação dos novos projetos. Sobre os controlos que utilizaram nos projetos anteriores, a encriptação foi o mais utilizado a considerar pelas respostas. Infelizmente existe profissionais que não utilizaram nenhum controlo nos projetos, deixando em aberto um perigo grande de ocorrer alguma falha de segurança futura mais facilmente do que os que adotaram algum tipo de controlo de proteção na aplicação.

Os direitos de acesso aos dados pessoais, atualização e eliminação são contemplados considerando as respostas, porém o direito de portabilidade e esquecimento é ainda negligenciado. Sobre o backup da aplicação e da base de dados verifica-se que ainda existe uma percentagem grande de profissionais que não fazem uso desta prática.

A maioria das respostas afirma ser importante um processo para facilitar o *design* e a conceção da aplicação para alinhar o SDLC ao RGPD, porém ainda há um número grande que não tem o conhecimento da importância dessa prática levando a um desalinhamento entre as aplicações que recolhem e tratam dados pessoais e o RGPD. Empresas nestas situações podem ser mais penalizadas comparativamente a outras que adotem comportamentos mais seguros.

Esse inquérito foi muito enriquecedor ao trabalho, afirmando a grande importância de existir um processo para ajudar os programadores e os envolvidos nos projetos a terem um guião para alinhar as aplicações com o RGPD, garantindo que durante todas as fases do SDLC esses profissionais possam se orientar e aumentar o nível de segurança das suas aplicações com uma maior conformidade com o regulamento.

Capítulo 5

Processo de referência para o alinhamento entre o SDLC e o RGPD

Neste capítulo é apresentado um processo de referência que foca o alinhamento entre o ciclo de desenvolvimento de software e o RGPD. O processo é composto por seis procedimentos e documentos desenvolvidos para auxiliar a equipa de desenvolvimento durante a criação dos novos projetos e assim dotar o software dos requisitos essenciais para obtenção da privacidade nos dados pessoais. Com isso, o ciclo de desenvolvimento de software (SDLC) contará com os princípios e meios (controlos) que facultem a conceção e por defeito de acordo com o Regulamento Geral sobre a Proteção dos Dados. O resultado será o alinhamento do SDLC com o RGPD aumentando a segurança no desenvolvimento do software e a salvaguarda das organizações em cumprimento com o regulamento.

O processo contém um conjunto procedimentos, um para cada uma das seis fases do SDCL que corresponde ao Levantamento e Análise de Requisitos, Desenho, Implementação, Teste, Implantação e Manutenção do software. Cada procedimento faz o alinhamento como o RGPD e contempla documentos que servem de guião e suporte à informação que passa de fase para fase. Cada documento contém um número de versão, indicando que os mesmos podem ser reformulados em resultado de processos de melhoria contínua que podem determinar a revisão dos procedimentos.

Ao longo das próximas seções é apresentado os procedimentos com as suas atividades, sendo detalhada cada uma das fases e apresentados os documentos de suporte. Tratando-se de um alinhamento entre o SDLC e o RGPD, os documentos elaborados numa determinada fase do SDLC são passados à fase seguinte para ser tidos em consideração no processo de desenvolvimento do *software*. O processo é apresentado de forma integral no anexo B (tanto na versão portuguesa como na versão inglesa).

5.1. Levantamento e a Análise de Requisitos – SDLC e RGPD

O primeiro procedimento é referente a fase de Levantamento e Análise de Requisitos. Os Responsáveis por esse procedimento são o Analista de Sistemas e o DPO, porém no documento também deve constar a assinatura do gestor do projeto que acompanha a equipa durante toda a criação do software. Assim é recomendado nas outras fases que também deverão constar a assinatura do responsável por ela, do DPO e do gestor do projeto.

Como apresentado na Figura 5.1.1, no início da atividade do procedimento da fase levantamento e a análise dos requisitos, verifica se a aplicação lidará com dados pessoais ou sensíveis. Caso for

confirmado que não existe nenhum tipo de informação de identificação pessoal, seguirá para o fim do procedimento. Caso contrário, se a confirmação for positiva para a existência de dados pessoais ou sensíveis como por exemplo primeiro nome, último nome, nome completo, número de telemóvel, número do CC, número do passaporte, número de identificação fiscal, morada, estado civil ou outro tipo de informação pessoal, durante a análise da atividade desse procedimento, o primeiro passo é fazer a Avaliação de Impacto sobre a Proteção de Dados. No final da atividade será gerado o documento SDLC-RGPD-PRO1-Doc0001v1 com os detalhes da atividade assinado pelos responsáveis e com a data da realização do procedimento.

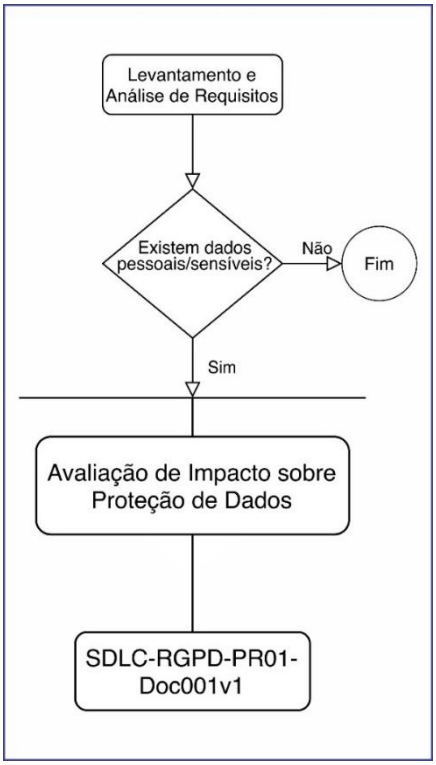


Figura 5.1.1 - Atividade de avaliação de impacto sobre proteção de dados

O segundo passo da atividade desse procedimento, tal como apresentado na Figura 5.1.2, é verificar se já existe algum modelo de consentimento explícito que possa ser usado para o projeto. Caso não exista, deverá ser assinalado a opção “Não” e introduzida a informação associada para elaborar o formulário de consentimento. Se positivo, assinalar a opção “Sim” deve-se indicar o formulário de consentimento. Estas opções são registadas no documento de consentimento explícito - SDLC-RGPD-PRO1-Doc002v1.

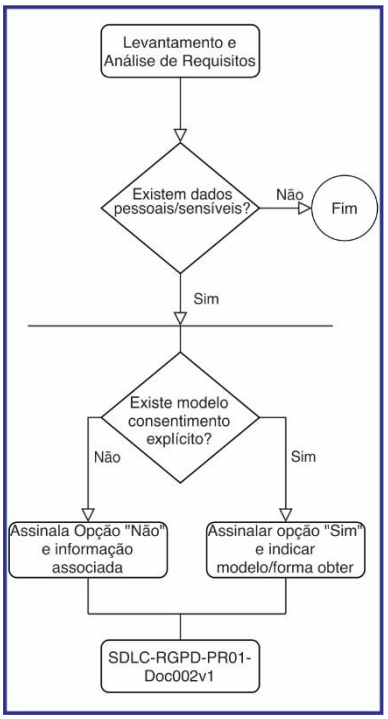


Figura 5.1.2 - Atividade para verificar se existe modelo de consentimento explícito

O próximo passo, como apresentado na Figura 5.1.3, é para determinar se os dados pessoais ou sensíveis a recolher e tratar já estão definidos e analisar se os mesmos são adequados ao projeto. Se os dados estivem definidos, completar os formulários e preencher o documento Dados a Recolher - SDLC-RGPD-PRO1-Doc003v1. Caso negativo, é registada a necessidade de fazer o levantamento dos dados a recolher para proceder ao preenchimento do respetivo formulário.

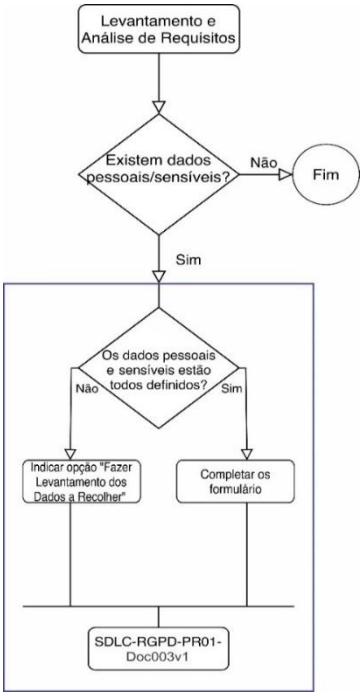


Figura 5.1.3 - Atividade para investigar a indicação dos dados pessoais ou sensíveis

O quarto ponto dessa fase, a atividade ilustrada na Figura 5.1.4, é o de apurar se irão existir diferentes perfis ou níveis de acesso de utilizador na aplicação. Caso não exista, deverá indicar tal no documento de Perfis. Se existir e se os mesmos já estiverem definidos, então deve-se completar o documento. Se não estiverem definidos os perfis / níveis de acesso à aplicação, recomenda-se realizar o levantamento para se proceder ao preenchimento do documento Perfis - SDLC-RGPD-PR01-Doc004v1.

A existência de dados pessoais a recolher e tratar na aplicação, com o cruzamento dos perfis/níveis de acesso à aplicação é determinante para a definição de uma atividade de mapeamento de dados que indica quem pode aceder a determinados dados pessoais por tipo de operação (leitura, atualização, eliminação, criação).

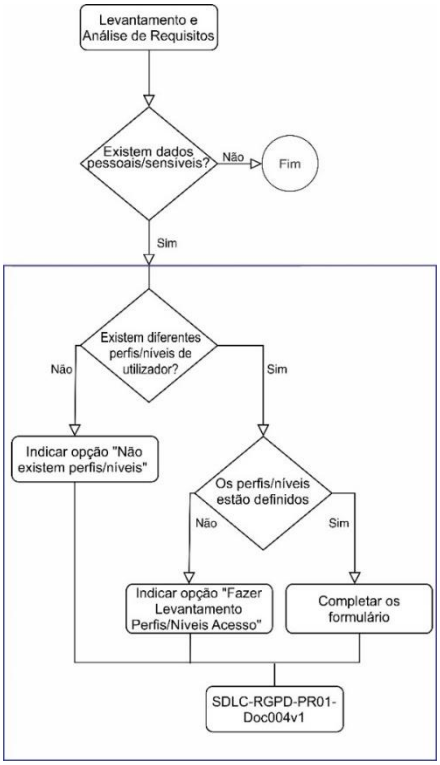


Figura 5.1.4 - Atividade para apurar se existem diferente perfis ou níveis de acesso

Ainda na primeira etapa do SDLC a próxima atividade, passa por averiguar, de acordo com a Figura 5.1.5, a existência de procedimentos que possibilitem aos titulares dos dados pessoais, exercerem seus direitos (acesso aos dados pessoais, pedido de portabilidade, pedido de esquecimento ou atualização). A disponibilização e forma de disponibilizar estes direitos são registados no formulário de Direito dos Titulares dos Dados, documento SDLC-RGPD-PR01-Doc005v1.

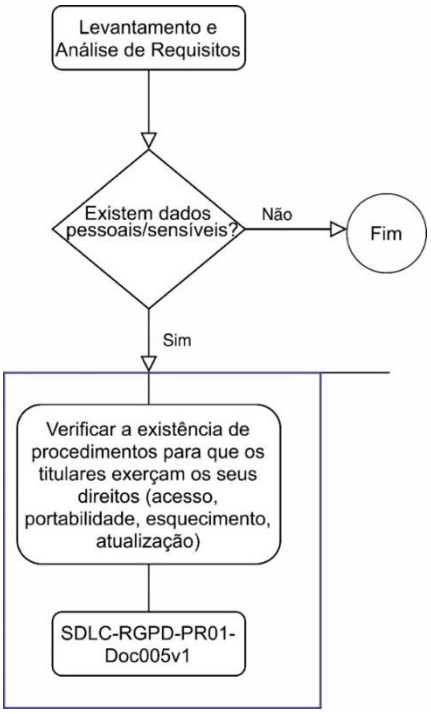


Figura 5.1.5 - Atividade para os titulares dos dados pessoais exercerem seus direitos

O último passo do procedimento RGPD alinhado com a primeira fase do SDLC consiste na atividade, tal como apresentado na Figura 5.1.6, em apurar se estão contemplados, a existência dos backups para a base de dados onde constam os dados pessoais. Confirmando a existência de backups, o plano deve ser apresentado no documento SDLC-RGPD-PR01-Doc006v1. Se os backups não estiverem definidos, refletir a questão no documento com a indicação do procedimento a adotar nessa situação.

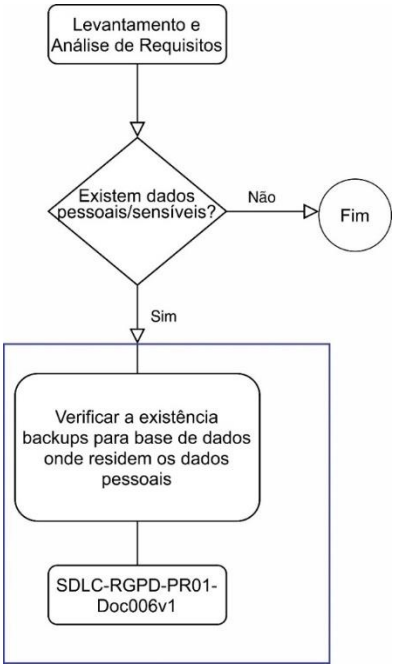


Figura 5.1.6 - Atividade para verificar a existência dos backups na base de dados

A Figura 5.1.7 apresenta todas as atividades do procedimento da primeira fase do SDLC levantamento e a análise de requisitos com todas as suas atividades.

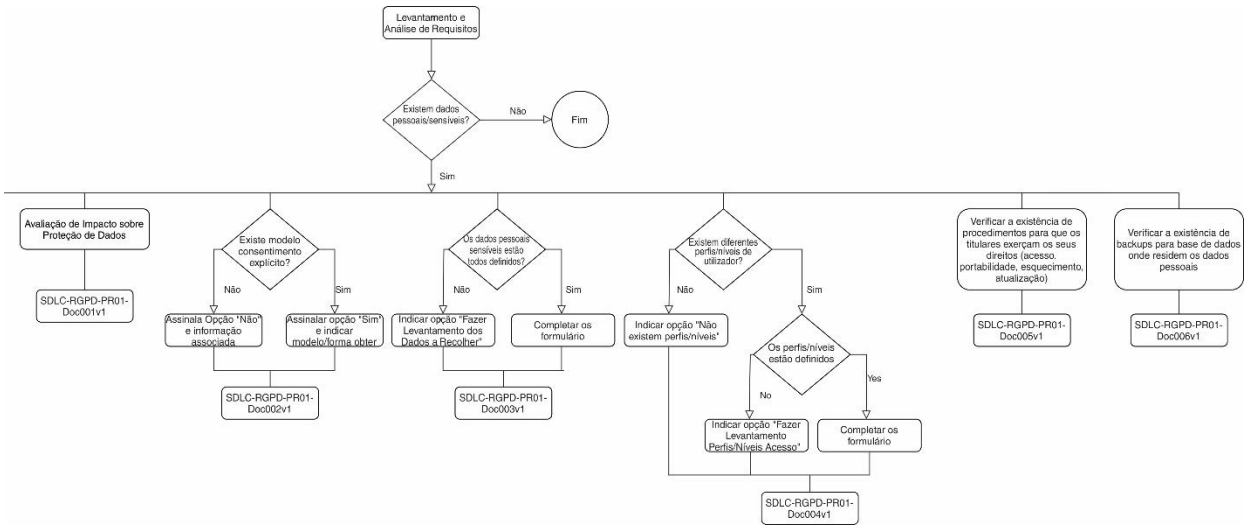


Figura 5.1.7 - Conjunto de atividades do procedimento Levantamento e Análise de Requisitos

Além dessas atividades da primeira fase do SDLC, também foram desenvolvidos os respetivos documentos para cada atividade. A Figura 5.1.8 tal como apresentado, refere-se à primeira página do documento de procedimento. Avaliação de Impacto sobre a Proteção de dados (AIPD) - SDLC-RGPD-PR01-Doc001v1 - o qual deve ser preenchido pelo analista responsável e o DPO envolvidos no projeto.

AVALIAÇÃO DE IMPACTO SOBRE PROTEÇÃO DE DADOS (AIPD)

1 - Âmbito da AIPD:

2 - Objetivo da avaliação de impacto

3 - Equipa e contactos dos responsáveis, indique:

Nome	Contato

4 - Operações de Tratamento de dados pessoais:

Contexto e finalidade do tratamento dos dados pessoais	
Ativos importantes que dependem de dados pessoais (componentes, sistemas, redes, papel)	
Acesso aos dados pessoais	<Será tratado pelo processo identificado no documento SDLC-RGPD-PR01-Doc004v1>
Descrição das operações de tratamento de dados pessoais	<Será tratado pelo processo identificado no documento SDLC-RGPD-PR01-Doc003v1>

5 - Avaliação das necessidades nas operações de processamento:

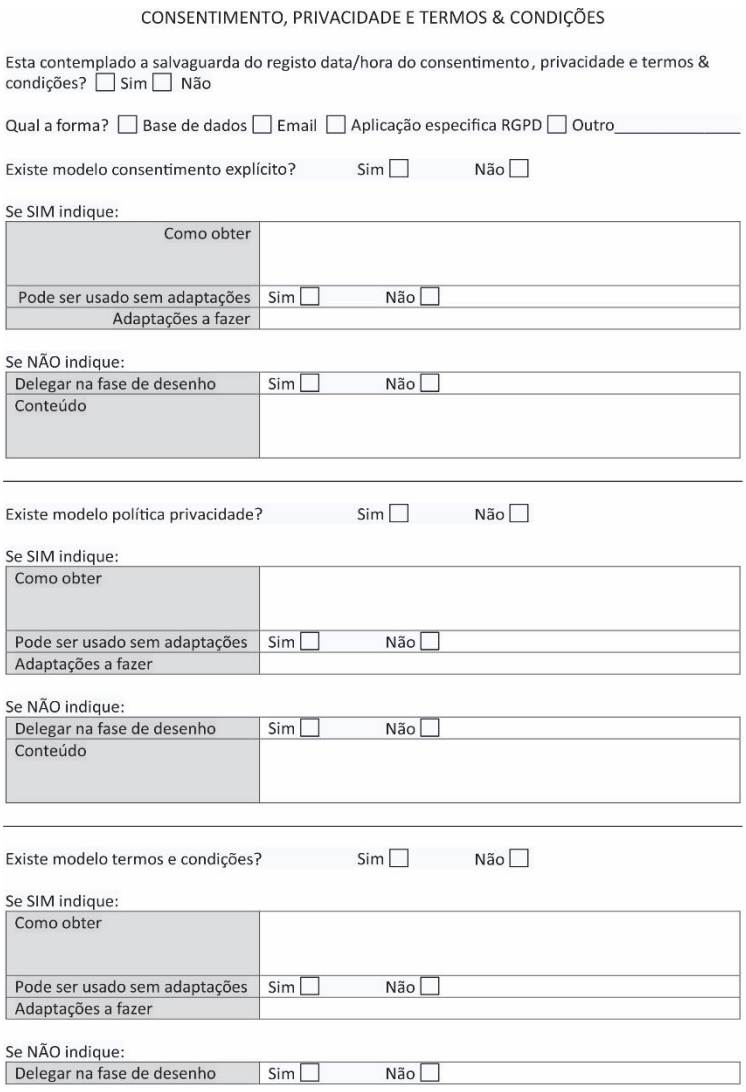
Medidas previstas para demonstrar a conformidade e necessidade do tratamento	

Figura 5.1.8 - Documento Avaliação de Impacto obre Proteção de dados (AIPD)

O documento Avaliação de Impacto obre Proteção de dados (AIPD) possui duas páginas com informações recolhidas na fase de início do projeto. Dentre as informações constam: uma descrição o tratamento de dados com a avaliação relativa à necessidade e proporcionalidade desse tratamento; uma análise de risco relativo aos direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos. O AIPD é um instrumento importante em matéria de responsabilização, uma vez que ajuda os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para acautelar riscos de forma adequada.

Em seguida o procedimento foca a avaliação e mitigação de riscos relacionados com: a violação da confidencialidade ou integridade; perda de dados; exercício dos direitos dos titulares de dados; possíveis impactos e ameaças e medidas para redução dos riscos com as descrições técnicas. Esta avaliação parte de uma análise de risco e contempla medidas de segurança e procedimentos para assegurar a proteção dos dados (descrição de medidas técnicas para assegurar a proteção) havendo no fim um campo para recomendações de melhoria.

O segundo documento criado da atividade a ser preenchido como mostra na Figura 5.1.9, é referente ao Consentimento, Privacidade e Termos & Condições - SDLC-RGPD-PR01-Doc002v1. Inicialmente ele verifica sobre a salvaguarda do registo de data e hora deles e a forma como foi feito. Em seguida começa os questionários sobre a existência ou não dos modelos deles, se podem ser usados sem adaptações ou se há alguma alteração a fazer. E se negativo recomenda-se ser delegado na próxima fase do desenho do projeto informando o conteúdo.



CONSENTIMENTO, PRIVACIDADE E TERMOS & CONDIÇÕES

Esta contemplado a salvaguarda do registo data/hora do consentimento, privacidade e termos & condições? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Existe modelo consentimento explícito? Sim ☐ Não ☐

Se SIM indique:

Como obter	
Pode ser usado sem adaptações	Sim ☐ Não ☐
Adaptações a fazer	

Se NÃO indique:

Delegar na fase de desenho	Sim ☐ Não ☐
Conteúdo	

Existe modelo política privacidade? Sim ☐ Não ☐

Se SIM indique:

Como obter	
Pode ser usado sem adaptações	Sim ☐ Não ☐
Adaptações a fazer	

Se NÃO indique:

Delegar na fase de desenho	Sim ☐ Não ☐
Conteúdo	

Existe modelo termos e condições? Sim ☐ Não ☐

Se SIM indique:

Como obter	
Pode ser usado sem adaptações	Sim ☐ Não ☐
Adaptações a fazer	

Se NÃO indique:

Delegar na fase de desenho	Sim ☐ Não ☐

Figura 5.1.9 - Documento de Consentimento, Privacidade e Termos & Condições

Outro documento importante é o tal apresentado na Figura 5.1.10, de Recolha e Tratamento de Dados - Especificação de Dados - SDLC-RGPD-PR01-Doc003v1 - o qual é feito a recolha dos dados pessoais / sensíveis a tratar. Foi sugerido uma lista com alguns campos de exemplo, na outra coluna se serão, ou não recolhidos ou se será definido posteriormente e o mais importante a justificação do uso desse dado na aplicação.

RECOLHA E TRATAMENTO DE DADOS – ESPECIFICAÇÃO DE DADOS

Dados pessoais/sensíveis e recolher e tratar

Campo	Recolher S/N?	Justificação
Primeiro Nome	Sim ☐ Não ☐ a definir ☐	
Último Nome	Sim ☐ Não ☐ a definir ☐	
Nome completo	Sim ☐ Não ☐ a definir ☐	
Número de telemóvel	Sim ☐ Não ☐ a definir ☐	
Número do CC	Sim ☐ Não ☐ a definir ☐	
Número do passaporte	Sim ☐ Não ☐ a definir ☐	
Número de Identificação Fiscal	Sim ☐ Não ☐ a definir ☐	
Morada	Sim ☐ Não ☐ a definir ☐	
Filiação Política	Sim ☐ Não ☐ a definir ☐	
Religião	Sim ☐ Não ☐ a definir ☐	
Doenças	Sim ☐ Não ☐ a definir ☐	
Idade	Sim ☐ Não ☐ a definir ☐	
Gênero	Sim ☐ Não ☐ a definir ☐	
Email	Sim ☐ Não ☐ a definir ☐	
Data Nascimento	Sim ☐ Não ☐ a definir ☐	
...	Sim ☐ Não ☐ a definir ☐	

Figura 5.1.10 - Documento Recolha e Tratamento de Dados -Especificação de Dados

Nessa primeira fase, também foi criado o documento Perfis/Níveis Controlo de Acessos - SDLC-RGPD-PR01-Doc004v1 - bem como Figura 5.1.11, que determina de acordo com o perfil, o nível de acesso do utilizador se será sem limite, com um limite ou a definir depois e um campo de observações sugerido para cada perfil.

Se SIM indique os perfis/níveis aplicacionais

Perfil	Nível acesso	Observações
Admin	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	
...	Ilimitado ☐ Limitado ☐ a definir ☐	

Figura 5.1.11 - Documento Perfis/Níveis Controlo de Acessos

O documento seguinte elaborado de acordo com a Figura 5.1.12, reflete os Direitos dos Utilizadores - SDLC-RGPD-PR01-Doc005v1. Ele começa abordando sobre a contemplação da salvaguarda com registo da data e hora dos direitos dos utilizadores, em seguida a forma, se foi por base de dados, email, aplicação específica do RGPD ou outro tipo especificando o mesmo.

Na tabela desse documento é informado alguns dos principais direitos dos titulares dos dados, como o direito de acesso, portabilidade, esquecimento e atualização, porém deixando outros campos para outros direitos que possam ser acrescentados nesse documento. É questionado sobre o estado de cada direito, se já existe suporte, se deverá ser criado ou se é desnecessário para o projeto. Posteriormente uma coluna para assinalar o formato, dadas as opções de email, portal, formulário aplicacional, aviso, incluídos nos avisos legais ou outro tipo e com um campo observações para cada direito.

DIREITOS DOS UTILIZADORES

Está contemplado a salvaguarda do registo data/hora dos direitos dos utilizadores? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Direito	Estado	Formato	Observações
Acesso	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Portabilidade	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Esquecimento	já existe suporte ☐ a criar suporte ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Atualização	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	

Figura 5.1.12 - Documento Direitos dos Utilizadores

O último documento desenvolvido dessa etapa do SDLC, tal como Figura 5.1.13, destina-se aos Backups dos Dados Pessoais – Data At Rest - SDLC-RGPD-PR01-Doc006v1. Inicialmente é proposto analisar se existe alguma política de backup na organização e se devem ser feitos backups dos dados que serão criados no âmbito da aplicação. Se afirmativo, sugere-se descrever o plano de backup, determinando o tipo (total - cópia completa dos dados, incremental – cópia dos dados alterados desde o último backup, *archive logs* – backup das transações efetuadas na base de dados ou outro), também a periodicidade (diário, semanal, mensal ou outro), tipo (*online* ou *offline*), a segurança (cifrados, não cifrados) e o local de armazenamento (*onsite* ou *offsite*).

BACKUPS DOS DADOS PESSOAIS – DATA AT REST

Existem políticas de backup na organização: Sim ☐ Não ☐ N.A. ☐

Devem ser feitos backups dos dados a criar no âmbito da aplicação: Sim ☐ Não ☐

Se SIM descreva o plano de backups:

Tipo	Periodicidade	Tipo	Segurança	Local
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Outro		Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐

Figura 5.1.13 - Documento Backups dos Dados Pessoais

5.2. Fase de Desenho – SDLC e RGPD

O segundo procedimento criado é referente a fase Desenho do SDLC a incluir o RGPD de acordo com as informações recolhidas na análise de requisitos da fase anterior. O Responsável por esse procedimento é o Desenhista, porém no documento também deve constar a assinatura do DPO e do gestor do projeto que acompanham a equipa durante toda a criação do software.

A primeira atividade do procedimento dessa fase seguindo o documento SDLC-RGPD-PR01-Doc001v1 refere-se ao Consentimento. Nele é verificado se já existe modelo de consentimento (fase anterior). Se não existir o modelo, é sugerido/desenhado dando lugar ao preenchimento do documento em questão. Caso exista, na próxima condição é sugerido verificar se ele pode ser usado sem adaptações. Se positivo, finaliza o procedimento. Do contrário, indica-se o preenchimento do documento de consentimento SDLC-RGPD-PRO2-Doc0001v1, tal como ilustrado na Figura 5.2.1.

Continuando o procedimento dessa fase os passos detalhados do Consentimento se repetem semelhantes para as atividades de Privacidade e também para os Termos e Condições da aplicação exigidas pelo RGPD. No final dessas duas atividades são gerados os documentos SDLC-RGPD-PRO2-Doc0002v1 e SDLC-RGPD-PRO2-Doc0003v1.

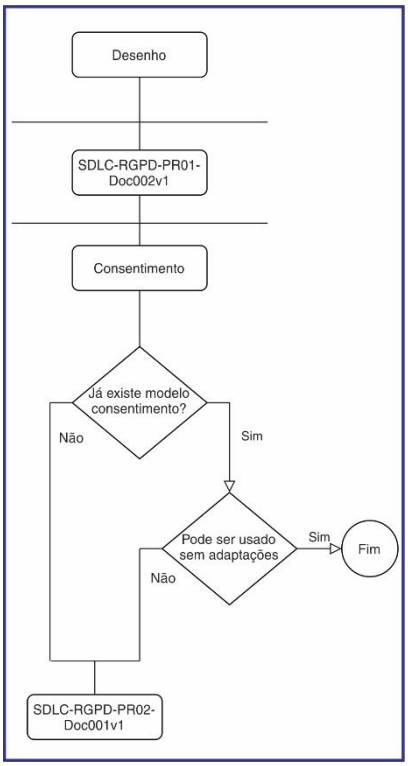


Figura 5.2.1 - Atividade consentimento da fase Desenho

Outro passo das atividades que foi construído nessa segunda fase do SDLC foi de acordo com às informações recolhidas nos documentos Recolha e Tratamento de Dados – Especificação de Dados que corresponde ao SDLC-RGPD-PRO1-Doc0003v1 e o Perfis/Níveis Controlo de Acessos correspondente ao SDLC-RGPD-PRO1-Doc0004v1. Essa atividade, ilustrada na Figura 5.2.2, começa verificando se ambos documentos foram preenchidos na recolha de requisitos e se estão definidos. A partir deles é preenchida a Matriz de Acesso (Data Mapping) refletida no documento SDLC-RGPD-PRO2-Doc0004v1.

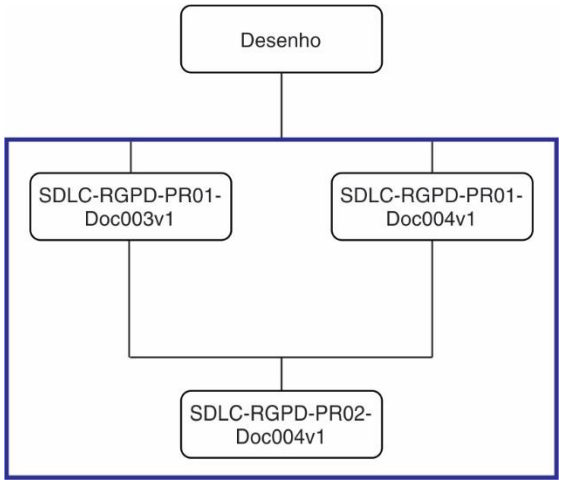


Figura 5.2.2 - Atividade para construção da matriz de acesso / dados (data mapping)

Seguindo os próximos passos do procedimento do desenho, é apresentado a atividade na Figura 5.2.3, que começa por verificar se o documento Direito dos Titulares dos Dados - SDLC-RGPD-PR01-Doc005v1 - foi definido no levantamento dos requisitos. Caso afirmativo orienta-se completar o documento Direito de Acesso dos Titulares de PII, documento SDLC-RGPD-PRO2-Doc0005v1.
Para os outros direitos dos titulares de dados como o direito de Portabilidade, Esquecimento, Atualização ou outro que o RGPD obriga o cumprimento, orienta-se seguir a mesma base dessa atividade realizada no direito de acesso. No final é gerado um documento para preenchimento de cada uma das atividades desses outros direitos, documentos SDLC-RGPD-PRO2-Doc0006v1, SDLC-RGPD-PRO2-Doc0007v1, SDLC-RGPD-PRO2-Doc0008v1 e SDLC-RGPD-PRO2-Doc0009v1.

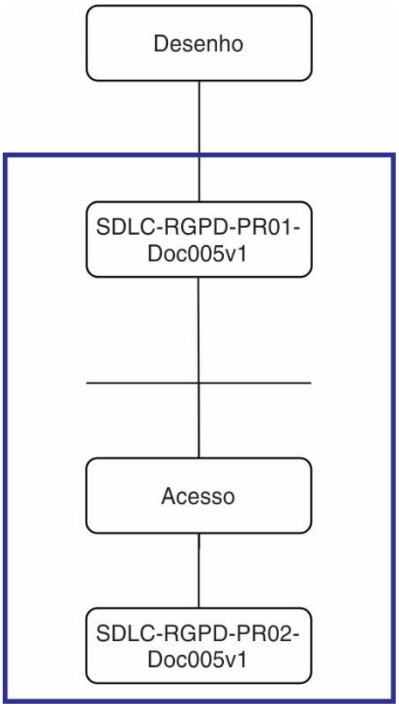


Figura 5.2.3 - Atividade referente ao direito do titular dos dados de acesso às suas PII

A última parte do procedimento do desenho, ilustrado na atividade da Figura 5.2.4, verifica se houve a definição do documento da fase anterior dos Backups dos Dados Pessoais – Data At Rest – documento SDLC-RGPD-PR01-Doc006v1. Após essa análise é direcionado para confirmar as informações do Backup dos Dados Pessoais dando lugar ao documento SDLC-RGPD-PR02-Doc0010v1.

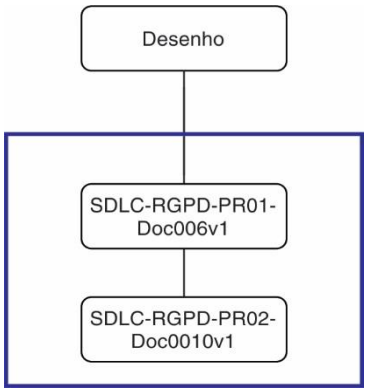


Figura 5.2.4 - Atividade referente ao backup dos dados pessoais

O procedimento da fase SDLC desenho, com as atividades completas é ilustrado na Figura 5.2.5. São também apresentados os documentos que detalham as orientações de cada etapa. Nessa segunda fase do SDLC o desenhista responsável realiza o preenchimento dos documentos para orientar o desenvolvedor na implementação do software alinhando o SDLC e o RGPD.

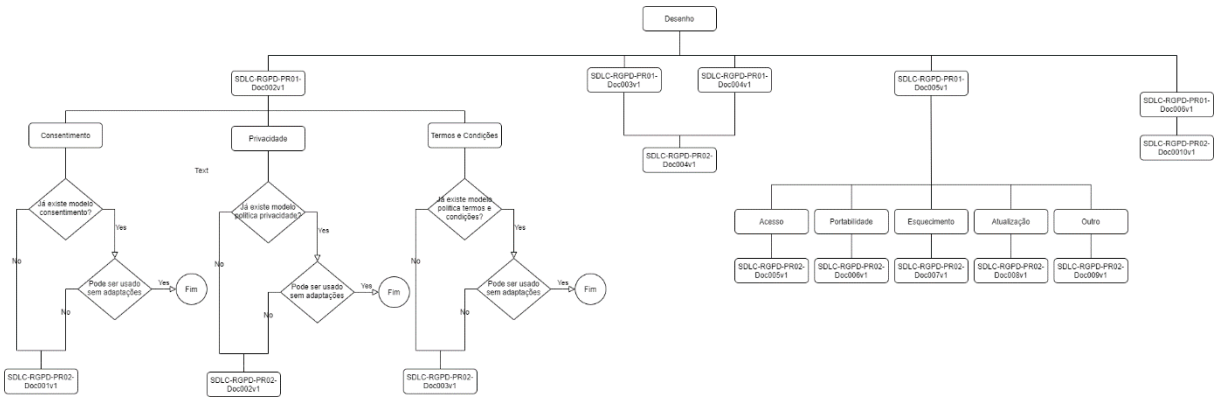


Figura 5.2.5 - Conjunto de atividades do procedimento Desenho

O primeiro documento dessa fase, tal como mostrado na Figura 5.2.6, Consentimento - SDLC-RGPD-PR02-Doc001v1 - inicia com o questionário para averiguar se está sendo contemplado data e hora do consentimento e de que forma (base de dados, email, aplicação específica RGPD ou outro) esse registo do consentimento será guardado. Também verifica se há um modelo de consentimento explícito e se ele pode ser usado sem adaptações. Em seguida apresenta o quadro onde é indicado colocar o *mockup*, texto, desenho do formulário ou página que será desenvolvido.

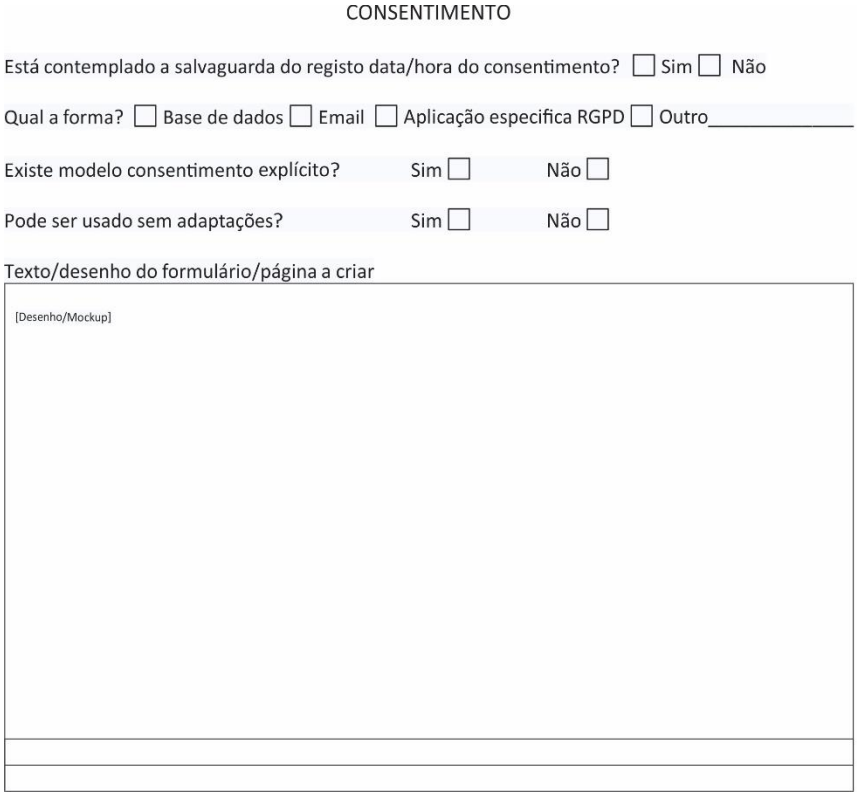


Figura 5.2.6 - Documento Consentimento

Assim, o circuito da atividade do Consentimento é semelhante para as atividades da Privacidade e também dos Termos e Condições da aplicação, os documentos também possuem estrutura análoga para ambos, porém as especificações deverão ser de acordo com o que cada um deles se refere. Por isso, foram criados documentos para cada um deles que acompanhará o anexo desse trabalho.

Outro documento criado e também com grande relevância ao projeto nessa fase de desenho, tal como na Figura 5.2.7, refere-se a Matriz de Acesso (Data Mapping) – documento SDLC-RGPD-PR02-Doc004v1. Ele é completado seguindo os documentos gerados na fase anterior Recolha e Tratamento de Dados – Especificação de dados, SDLC-RGPD-PR01-Doc003v1 e o Perfis / Níveis Controlo de Acessos, SDLC-RGPD-PR01-Doc004v1 com as informações que são recolhidas nessa primeira etapa.

MATRIZ DE ACESSOS / DADOS (DATA MAPPING)

INSTRUÇÕES:
Especificar os campos da BD relativos aos dados pessoais/sensíveis na linha 6
Especificar os utilizadores/perfis na coluna A

Completar com S/N sendo "S" indicação de operação permitida sobre os campos pelo utilizador/perfil e "N" a indicação de acesso proibido/desnecessário do utilizador/perfil correspondente

Função / Campo e Operações	Primeiro Nome				Sobrenome				Último nome				Telefone				Morada				Email		
	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U
admin		S		S				S				S		S		S				S		S	
rh				S				S				S				S				S			
inf				S				N				N				N				N			
ana@xpto.com				N				N				N				N				N			
manuel@xpto.com				S				N				N				S				N			

Figura 5.2.7 - Documento referência para criação da Matriz de Acessos

O documento SDLC-RGPD-PR02-Doc004v1possui as instruções para preenchimento, as quais são para especificar os campos da base de dados relativos aos dados pessoais e sensíveis, especificar os utilizadores de acordo com o seu perfil de acesso. E considerando as operações típicas CRUD, recomenda-se definir os acessos permitidos ou negados por utilizador ou perfil de utilizadores. O preenchimento deste documento será muito útil para a fase de desenvolvimento, onde o controlo de acessos granular será implementado, dando acesso ou inibindo o acesso à informação pessoal por utilizador consoante a matriz de acessos definida.

Ainda na fase do desenho também foi criado o documento para dar suporte aos direitos dos utilizadores. O documento Direito dos titulares de PII – Acesso SDLC-RGPD-PR02-Doc005v1 seguiu os dados recolhidos no levantamento de requisitos Direito dos Utilizadores – documento SDLC-RGPD-PR01-Doc005v1, como exibido na Figura 5.2.8. O mesmo se aplica aos outros documentos relativos aos direitos dos titulares dos dados que o RGPD obrigada, como Portabilidade, Esquecimento, Atualização e outro.

A atividade inicia com a abordagem a fim de verificar se está sendo contemplado a salvaguarda do registo data/hora do consentimento, questionando também a forma como foi feita (base de dados, email, aplicação específica RGPD ou outro com a especificação). Também verifica o estado em que se encontra, se já existe suporte, se precisa criar ou se é desnecessário.

DIREITOS DOS TITULARES DE PII – **ACESSO**

Está contemplado a salvaguarda do registo data/hora do consentimento? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação específica RGPD ☐ Outro_____

Estado
já existe suporte ☐ a criar ☐ desnecessário ☐

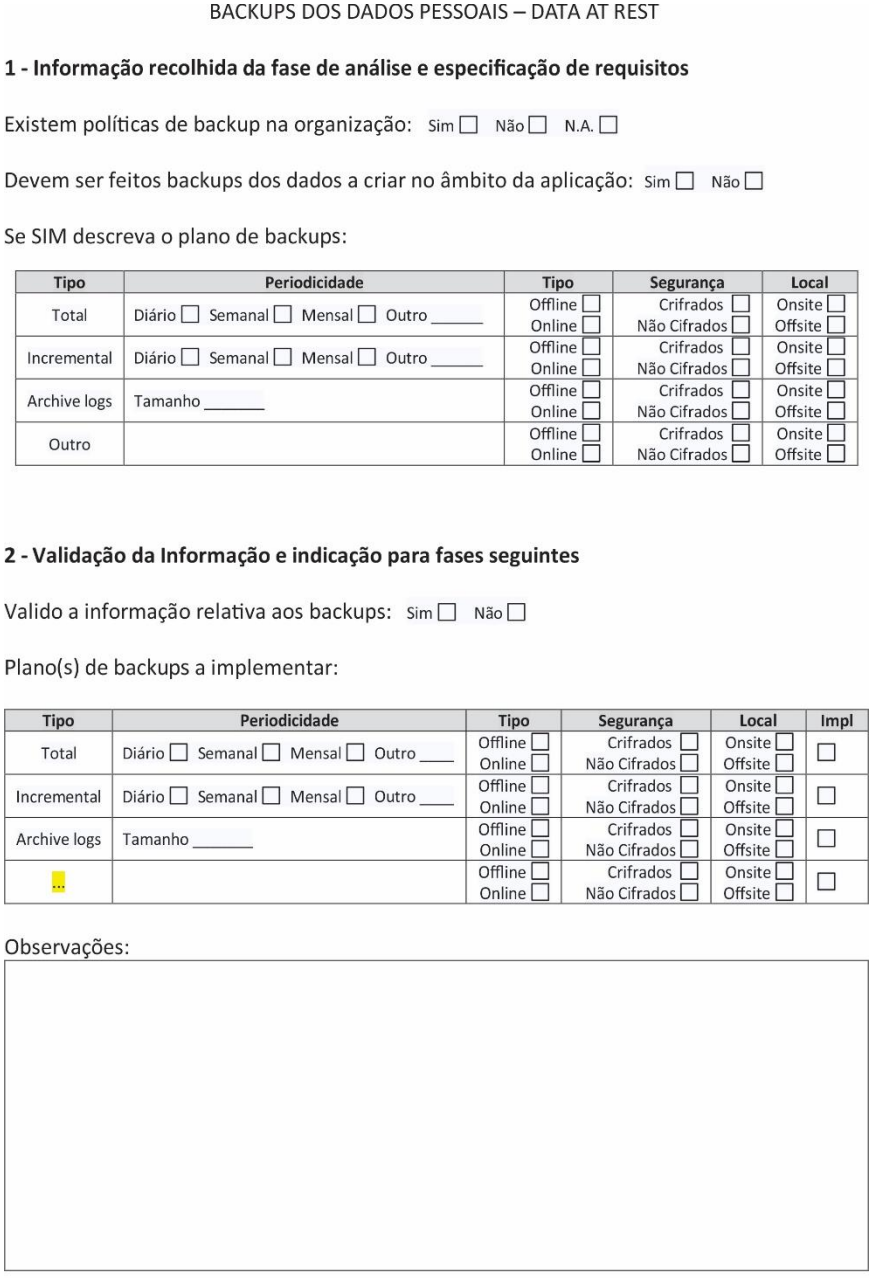
Formato		**Desenho/Mockup/Descrição**
Email	☐	<Indicar o endereço de email através do qual os utilizadores podem efetuar um pedido de acesso à sua PII. Indicar se é para incluir a existência desse endereço de email algum local da aplicação (Menu | termos e condições | privacidade | ...). O email poderá ainda ser desenhado/especificado para o efeito.>
Portal	☐	<Indicar caso já exista o portal/site da empresa através do qual os utilizadores podem efetuar um pedido de acesso à sua PII. Indicar se é para incluir a existência desse portal/site em algum local da aplicação (Menu | termos e condições | privacidade | ...)>
Formulário aplicacional	☐	<Desenhar/especificar o formulário aplicacional a incluir na aplicação que permita, através do mesmo, aos titulares dos dados efetuar um pedido de acesso à sua PII>
Aviso	☐	<Especificar o aviso (página) a apresentar aos utilizadores que pretendam efetuar um pedido de acesso à sua PII ou então a forma como o programador deverá enquadrar tal pedido na aplicação>
Incluído nos avisos legais	☐	<Este caso aplica-se quando a forma de efetuar um pedido de acesso à PII está incluída nos avisos legais podendo ainda ser descrita a forma como o programador deverá enquadrar tal na aplicação>
Outro _____ _____	☐	

Figura 5.2.8 - Documento Direitos dos Titulares de PII – Acesso

Tal como se pode ver pela Figura 5.2.8 são apresentados possíveis formatos de sugestão (emails, portal, formulário aplicacional, aviso, incluído nos avisos legais ou outro com a especificação) para serem definidos nessa fase, com desenho, construção de *mockup* e descrição dos procedimentos a realizar durante a implementação da aplicação atingindo as exigências do RGPD.

No desenho também foi desenvolvido o documento Backups dos Dados Pessoais – Data At Rest SDLC-RGPD-PR02-Doc0010v1, ilustrado na Figura 5.2.9, para preencher às informações que foram recolhidas na análise e especificação de requisitos guardadas anteriormente no documento SDLC-RGPD-PR01-Doc006v1. Se o documento para recolha das informações do backup não estiver preenchido na fase anterior então inicia-se questionando a existência de políticas na organização e se devem ser feitos

backups dos dados que serão criados no âmbito da aplicação. Se afirmativo o desenhista é orientado a descrever o plano de backup, definindo o tipo (total, incremental, *archive logs* ou outro), a periodicidade (diário, semanal, mensal ou outro) que será realizado, juntamente com o tipo (*online* ou *offline*), o tipo de segurança (cifrado ou não cifrado) e o local (*onsite* ou *offsite*).



BACKUPS DOS DADOS PESSOAIS – DATA AT REST

1 - Informação recolhida da fase de análise e especificação de requisitos

Existem políticas de backup na organização: Sim ☐ Não ☐ N.A. ☐

Devem ser feitos backups dos dados a criar no âmbito da aplicação: Sim ☐ Não ☐

Se SIM descreva o plano de backups:

Tipo	Periodicidade	Tipo	Segurança	Local
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Outro		Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐

2 - Validação da Informação e indicação para fases seguintes

Valido a informação relativa aos backups: Sim ☐ Não ☐

Plano(s) de backups a implementar:

Tipo	Periodicidade	Tipo	Segurança	Local	Impl
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro ____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro ____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
...		Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐

Observações:

Figura 5.2.9 - Documento Backups dos Dados Pessoais – Data At Rest

Neste documento, deve-se ainda preencher a validação das informações para as próximas fases do SDLC assinalando o campo implementado da tabela do item dois. Em seguida, há um quadro de observações, para preencher, caso necessário algum complemento para auxiliar durante a fase seguinte do projeto e ficar registado no documento.

5.3. Fase de Implementação – SDLC e RGPD

Na implementação também foram criados os circuitos das atividades e os documentos referentes a essa fase. A primeira parte da atividade tem como base os documentos da fase anterior.

Nessa fase de implementação do SDLC, deve-se incluir o RGPD na codificação do software seguindo as informações completadas na fase do desenho e com os documentos definidos nessa fase anterior. Através deles, será possível implementar na aplicação a forma dos titulares dos dados dar consentimento, concordar com os termos de privacidade e os termos e condições do serviço. O resultado da implementação será também alvo de um documento SDLC-RGPD-PR03-Doc001v1. Esta atividade é apresentada na Figura 5.3.1.

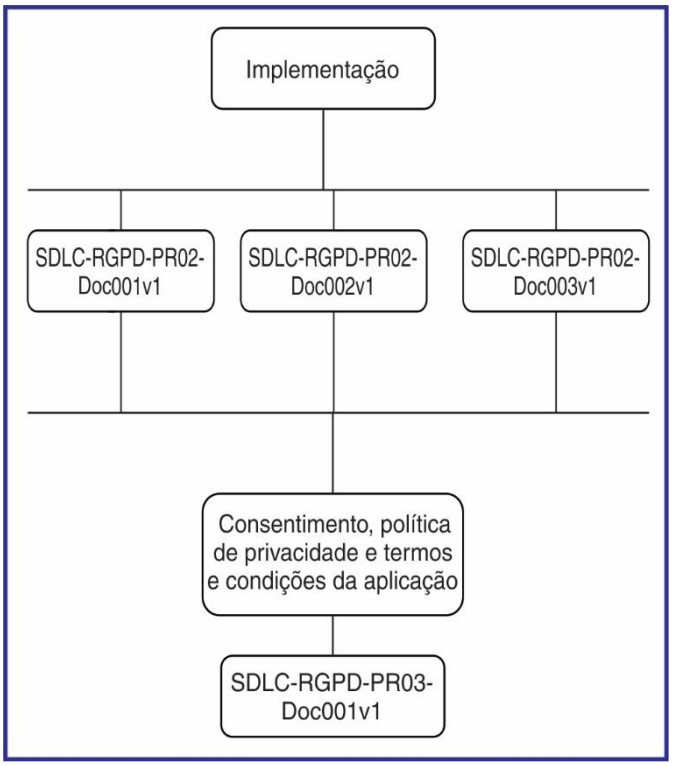


Figura 5.3.1 - Atividade implementação consentimento, política de privacidade e termos e condições

Outra atividade do procedimento de implementação, de acordo com a Figura 5.3.2, recorre ao documento definido anteriormente Matriz de Acesso SDLC-RGPD-PR02-Doc004v1, para realizar a implementação referente aos perfis e níveis de acessos ao que foram definidos no desenho. Na sequência essa atividade dita para especificar no documento Controlo de Acesso aos Dados pessoais as *queries* e vistas sobre a BD bem como controlos – documento SDLC-RGPD-PR03 Doc002v1 – que dão ou restringem o acesso aos dados considerando quem acede e o tipo de dados pessoais a aceder.

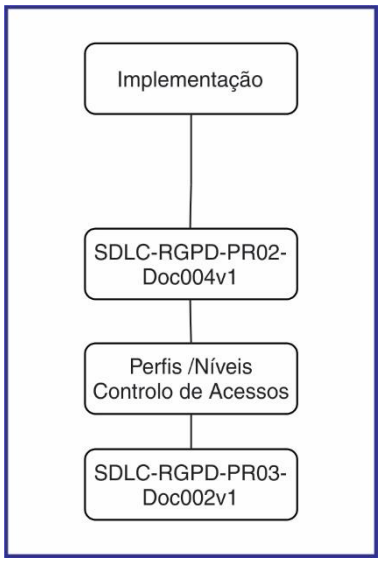


Figura 5.3.2 - Atividade controlo de acesso aos dados pessoais

Nessa fase também foi criado a atividade de pedido de acesso aos dados pessoais por parte dos titulares dos dados, como apresentada na Figura 5.3.3, seguindo o documento gerado do desenho Direitos dos Titulares de PII - SDLC-RGPD-PR02-Doc005v1. No final dessa atividade é gerada o documento Implementação do pedido de acesso aos dados - SDLC-RGPD-PR03-Doc003v1.

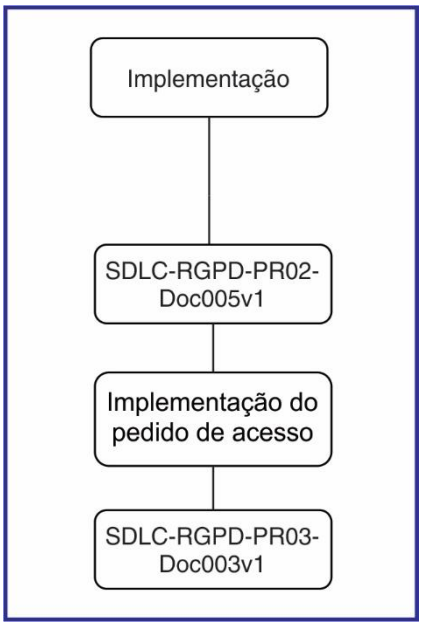


Figura 5.3.3 - Atividade de implementação do pedido de acesso

Outras atividades referentes aos direitos dos titulares como (direito de portabilidade, esquecimento, atualização e de outros pedidos) foram desenvolvidos nesse procedimento de implementação seguindo a analogia adotada na atividade detalhada acima.

O conjunto de atividades da fase implementação é apresentado na Figura 5.3.4. Para cada atividade desse procedimento foram criados os documentos que detalham as orientações de cada um. Nessa terceira fase do SDLC o desenvolvedor responsável realiza o preenchimento do documento para orientar a equipa de teste posteriormente.

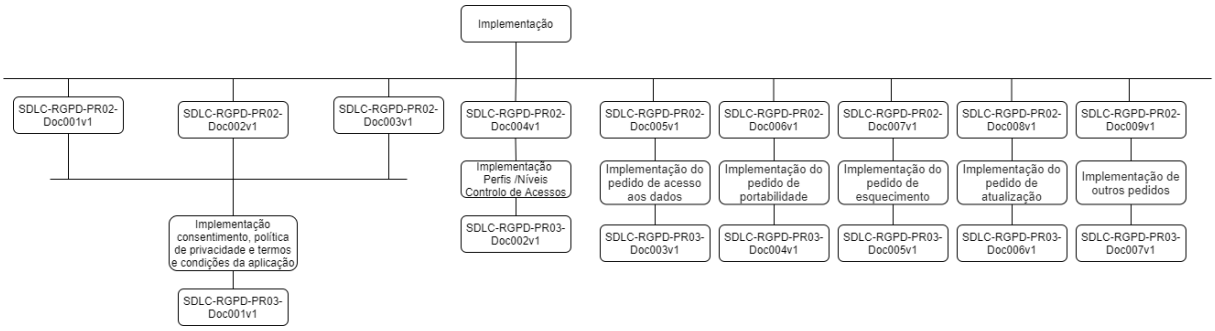


Figura 5.3.4 - Conjunto de atividades do procedimento Implementação

Assim como nas fases anteriores do SDLC, na fase de Implementação também foram criados os documentos correspondentes a cada etapa das atividades. Eles serão preenchidos após as validações da implementação.

O primeiro documento elaborado nessa etapa, tal como ilustrado na Figura 5.3.5 a primeira parte página dele, é o de Consentimento, Privacidade e Termos & Condições – documento SDLC-RGPD-PR03-Doc001v1. Este documento regista se foram implementados e de que forma são guardados o consentimento de recolha e tratamento PII, a política privacidade e os termos e condições e qual a forma que foram criados. Caso não esteja sendo armazenado essas informações, há um campo de observações onde pode ser indicado o motivo.

CONSENTIMENTO, PRIVACIDADE E TERMOS & CONDIÇÕES

Foi implementado o consentimento de recolha e tratamento PII? Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link	☐	Observações: indique aqui o link, *template* de email ou forma usada na implementação do consentimento de recolha e tratamento de dados pessoais. Caso tenha feito alterações ao modelo de consentimento recebido em fases anteriores indique aqui que alterações fez.
	Formulário	☐	
	Email	☐	
	Outro	☐	

Como está a ser guardado o consentimento?	
Não está a ser guardado	☐
Está a ser guardado	☐ (indicar abaixo como)
Observações:	

Se foi pedido e NÃO foi implementado, diga o porquê:

Foi implementado na aplicação o modelo política privacidade? Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link	☐	Observações: indique aqui o link, *template* de email ou forma usada na implementação/divulgação da política de privacidade em vigor na empresa. Caso tenha feito alterações ao modelo recebido em fases anteriores indique aqui que alterações foram feitas.
	Formulário	☐	
	Email	☐	
	Outro	☐	

Figura 5.3.5 - Consentimento, privacidade e termos & condições

O segundo documento elaborado dessa fase, como ilustrado na Figura 5.3.6, é o Controlo de acesso aos Dados Pessoais de acordo com Matriz de Acessos / Dados (Data Mapping) - SDLC-RGPD-PR03-Doc002v1. O documento regista se o controlo de acesso foi implementado de acordo com a Matriz de Acessos / Dados e se a Base de Dados foi protegida através de mecanismos de cifra. Também se o controlo de acessos foi implementado integralmente ou parcialmente. Em seguida, existem os campos para registar o utilizador / perfil e campo da BD, a query / vista implementada e o tipo de controlo adotado.

CONTROLO DE ACESSO AOS DADOS PESSOAIS
DE ACORDO COM MATRIZ DE ACESSOS / DADOS (DATA MAPPING)

O controle de acesso foi implementado de acordo com a Matriz de Acessos / Dados? Sim ☐ Não ☐ Parcialmente ☐ Não se aplica ☐

A BD está protegida através de mecanismos de cifra? Sim ☐ Não ☐

Se implementou integralmente ou parcialmente o controlo de acessos indique:

Utilizador/Perfil e Campo(s) da BD	Query/Vista implementada	Controlo adotado (ofuscação, anonimização, ...)
		Ofuscação ☐ Anonimização ☐ Outro ☐ _____
		Ofuscação ☐ Anonimização ☐ Outro ☐ _____
		Ofuscação ☐ Anonimização ☐ Outro ☐ _____
		Ofuscação ☐ Anonimização ☐ Outro ☐ _____

Figura 5.3.6 - Documento Controlo de acesso aos Dados Pessoais de acordo com Matriz de Acessos / Dados

Ainda na fase da implementação foram criados os documentos referentes aos direitos dos utilizadores. O documento ilustrado na Figura 5.3.7, Implementação do Pedido de Acesso aos Dados - SDLC-RGPD-PR03-Doc003v1 - regista se houve a implementação do direito de acesso e qual forma ocorreu. Caso não esteja implementado, há um campo para informar o motivo.

IMPLEMENTAÇÃO DO PEDIDO
DE ACESSO AOS DADOS

Foi implementado o **direito de acesso** aos dados do utilizador?

Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link		Observações: indique a forma usada na implementação do direito de acesso aos dados pessoais por parte dos utilizadores. Caso tenha feito alterações ao documento SDLC-RGPD-PR02-Doc005v1 indique aqui que alterações fez.
	Formulário		
	Email		
	Outro		

Se foi pedido e NÃO foi implementado, diga o porquê:

Figura 5.3.7 - Implementação do Pedido de Acesso aos Dados

O mesmo se aplica aos outros documentos elaborados relativos aos direitos dos titulares, como Portabilidade, Esquecimento, Atualização e outro.

5.4. Fase de Teste – SDLC e RGPD

Na fase de Testes do SDLC, o procedimento completo recomenda a verificação da implementação se atende ao RGPD através de uma auditoria de segurança, com enfoque na proteção das informações pessoais do titular dos dados.

A primeira atividade do procedimento teste, tal como ilustrado na Figura 5.4.1, considera o documento preenchido na fase de implementação, relativo ao Consentimento, Privacidade e Termos & Condições SDLC-RGPD-PR03-Doc001v1. Nesta fase e com base nos testes à aplicação completa-se o documento de validação e testes - SDLC-RGPD-PR04-Doc001v1. Este documento regista o resultados dos testes sobre o Pedido de Consentimento, Declaração de Privacidade e Termos e Condições permitindo verificar se a implementação ficou de acordo com às exigências do RGPD e se atende as fases anteriores do SDLC.

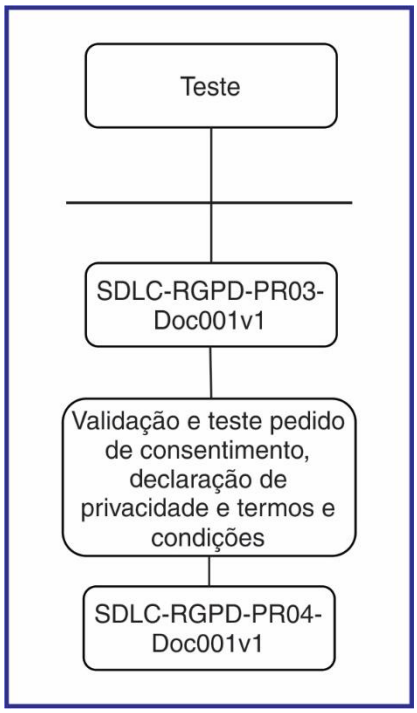


Figura 5.4.1 - Atividade validação e teste pedido de consentimento, declaração de privacidade e termo e condições

Outra atividade desse conjunto de atividades do procedimento teste, como apresentado na Figura 5.4.2, baseia-se no documento elaborado na fase de implementação Controlo de Acesso aos Dados Pessoais de acordo com a Matriz de Acessos - SDLC-RGPD-PR03-Doc002v1. Com base nos testes é preenchido o documento de validação e teste do Controlo de Acesso RGPD SDLC-RGPD-PR04-Doc002v1.

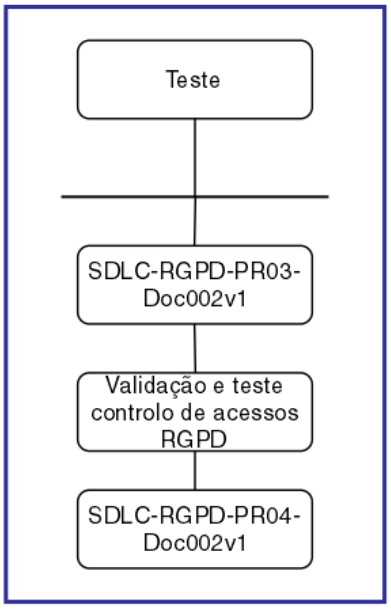


Figura 5.4.2 - Atividade validação e teste controlo de acessos

A próxima atividade é ilustrada na Figura 5.4.3. Esta busca como referência os documentos de implementação dos pedidos de Acesso aos Dados SDLC-RGPD-PR03-Doc003v1 , Portabilidade SDLC-RGPD-PR03-Doc004v1, Esquecimento SDLC-RGPD-PR03-Doc005v1 e Atualização SDLC-RGPD-PR06-Doc003v1, que foram desenvolvidos no projeto na fase anterior. Após os testes devem ser preenchido o documento de validação e teste dos direito dos utilizadores - SDLC-RGPD-PR04-Doc003v1.

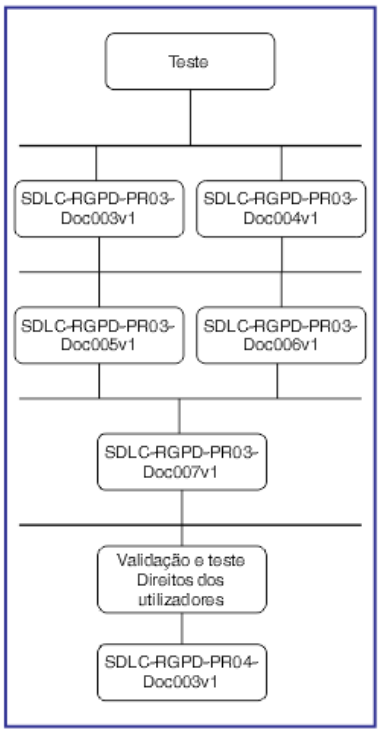


Figura 5.4.3 - Atividade validação e teste direitos dos utilizadores

O conjunto de atividades dessa fase teste é ilustrado na Figura 5.4.4. Cada atividade possui um documento que detalha às suas orientações. Nessa quarta fase do SDLC a equipa de teste faz o preenchimento e a validação dos documentos para colaborar com a próxima fase de implantação, ou caso o projeto retorne as fases anteriores se perceba o que correu menos bem.

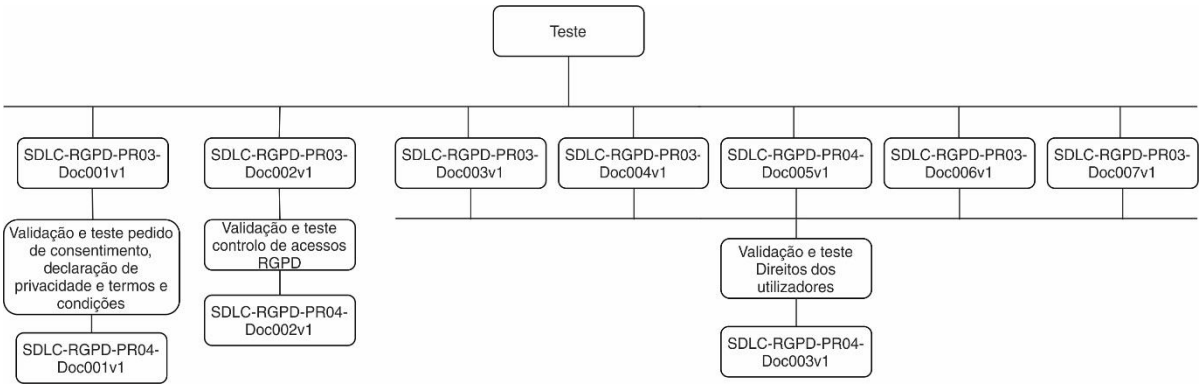


Figura 5.4.4 - Conjunto de atividades do procedimento Teste

Tal como nas fases anteriores do SDLC, na fase de Teste também foram preparados os documentos correspondentes a cada uma das atividades desse procedimento. Eles serão preenchidos após as validações dos testes realizados.

O primeiro documento contemplado nessa etapa, tal como ilustrado na Figura 5.4.5, é o de Validação e Teste Pedido de Consentimento, Declaração de Privacidade e Termos e Condições – documento SDLC-RGPD-PR04-Doc001v1. Este documento regista se pedido de consentimento ao titular de dados, a declaração de privacidade dos dados e os Termos e condições foram implementados, testados e se estão em conformidade ou não com o RGPD. Caso não esteja conforme, há um campo de observações onde é indicado o motivo da não conformidade.

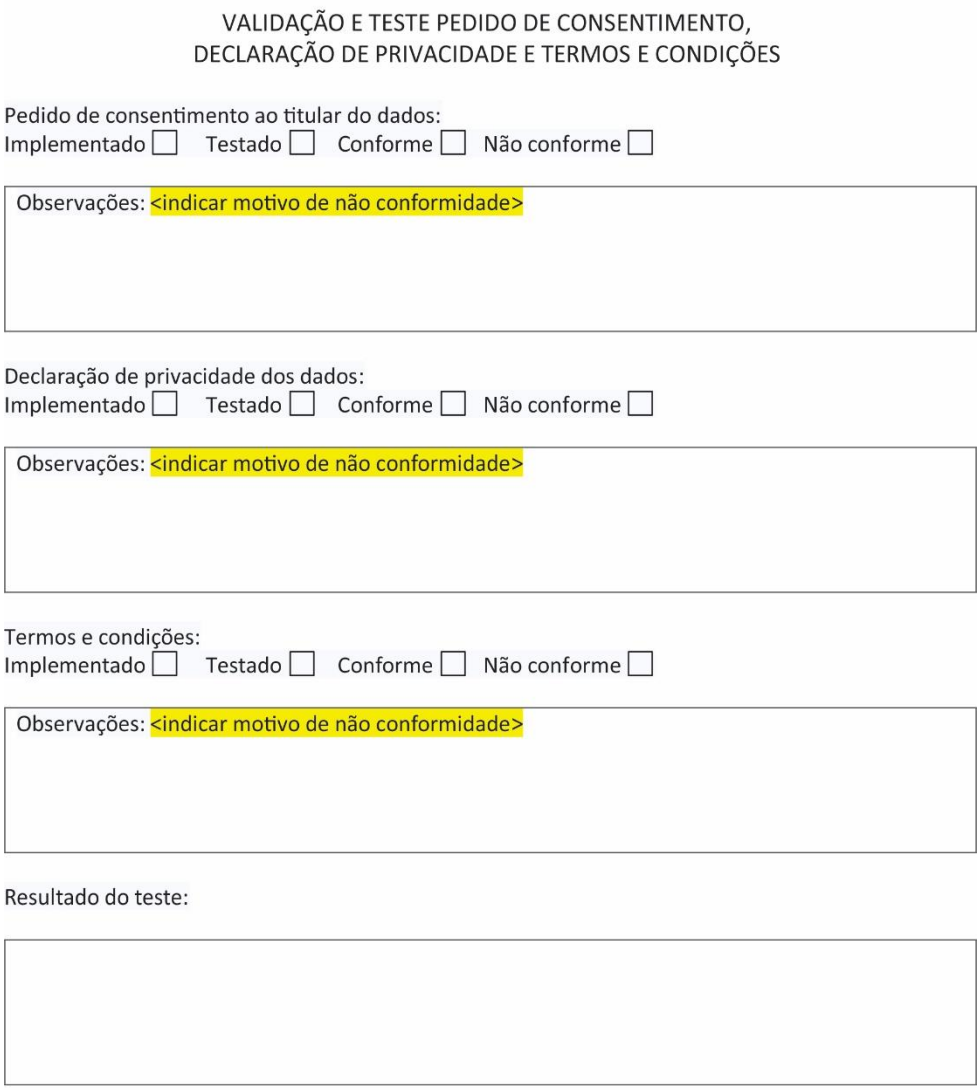


Figura 5.4.5 - Documento Validação e Teste Pedido de Consentimento, Declaração de Privacidade e Termos e Condições

O segundo documento elaborado dessa fase, como ilustrado na Figura 5.4.6, é o da Validação e Teste Controlo de Acessos RGPD - SDLC-RGPD-PR04-Doc002v1. Neste documento é apresentado a coluna para especificar o perfil / utilizador, o Formulário / Opção e o controlo adotado (ofuscação, anonimização ou outro, detalhando o tipo). Em seguida, há um campo para registar a validação do teste um campo de observações.

VALIDAÇÃO E TESTE CONTROLO DE ACESSOS RGPD

Perfil/ Utilizador	Formulário/Opção	Controlo adotado (ofuscação, anonimização, ...)	Validação/Teste	Observações
		Ofuscação ☐ Anonimização ☐ Outro ☐ __________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ __________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ __________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ __________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	

Figura 5.4.6 - Documento Validação e Teste Controlo de Acessos RGPD

O último documento dessa fase, apresentado na Figura 5.4.7, refere-se à Validação e Teste Direitos dos Utilizadores – documento SDLC-RGPD-PR04-Doc003v1. O documento é preenchido após realizar os testes aos direitos dos utilizadores (acesso, portabilidade, esquecimento, atualização ou outro). A validação dos procedimentos é registada nesse documento e assinalado se foram implementados na aplicação, testado e se está ou não conforme ao RGPD. Há um campo observação para acompanhar as respostas.

VALIDAÇÃO E TESTE DIREITOS
DOS UTILIZADORES

Pedido de **acesso** aos dados pessoais:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações:

Pedido de **portabilidade** dos dados pessoais:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações:

Pedido de **esquecimento** dos dados pessoais por parte do titular dos dados:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

...

Figura 5.4.7 - Primeira parte do documento Validação e Teste Direitos dos Utilizadores

5.5. Fase de Implantação – SDLC e RGPD

O procedimento da fase de implantação inicia após passar pela auditoria do teste em conformidade com o RGPD. Nessa fase o primeiro passo envolve a Gestão de Configurações das informações de identificação pessoal (PII) e aspetos relativos à Hospedagem da Aplicação, atividade ilustrada na Figura 5.5.1 que gera o documento SDLC-RGPD-PR05-Doc001v1.

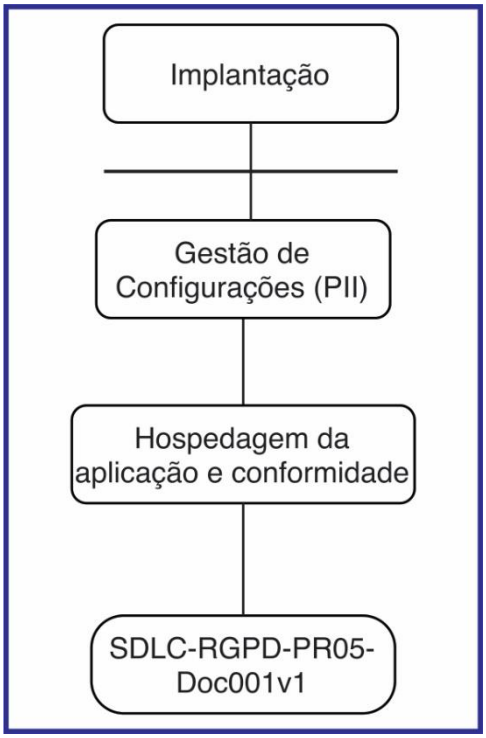


Figura 5.5.1 - Atividade hospedagem da aplicação e conformidade

A atividade continua com a Gestão de Configuração (PII), com referência ao documento da fase de desenho relativo aos Backups dos Dados Pessoais - SDLC-RGPD-PR02-Doc0010v1. Este documento suporta a implantação dos Backups e na sequência da implementação deve ser alimentado o documento de Backups da implantação SDLC-RGPD-PR05-Doc002v1.

Outro que também segue a mesma lógica da estrutura anterior é o do Logging e Monitorização dos dados pessoais - SDLC-RGPD-PR05-Doc003v1. Nesta fase o objetivo é verificar a se estão de acordo com o regulamento e o resultado da verificação deve ser registado no documento respetivo.

A próxima atividade da fase de implantação é apresentado na Figura 5.5.2. Esta atividade baseia-se na verificação do documento gerado na fase de Teste, mais propriamente na validação e teste do Controlo de Acessos RGPD – documento SDLC-RGPD-PR04-Doc002v1. Com base numa auditoria aplicacional

deve-se proceder ao registo do documento da implantação verificação e auditoria de segurança (PII) (Smoke Tests PRD) identificado como SDLC-RGPD-PR05-Doc004v1.

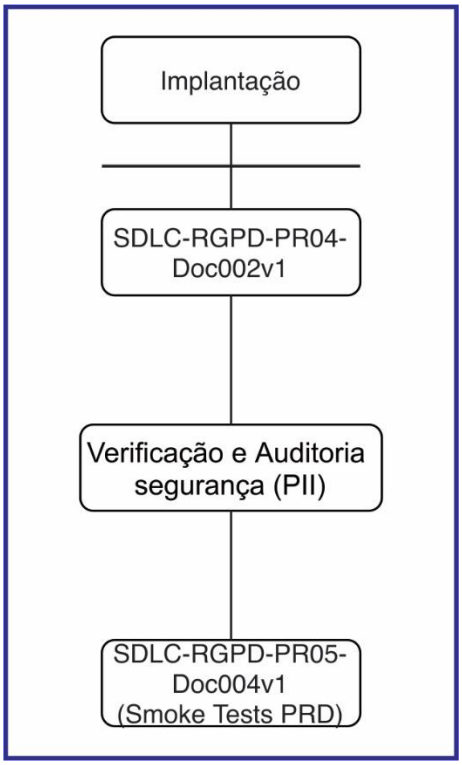


Figura 5.5.2 - Atividade verificação e auditoria segurança (PII)

A última atividade do procedimento dessa fase, tal como ilustrado na Figura 5.5.3, sugere o preenchimento do documento Solução Data Loss Prevention (DLP), para verificar se existe alguma solução na aplicação relativo ao DLP. Caso exista o Setup DLP (PII) deve ser guardado no documento SDLC-RGPD-PR05-Doc005v1.

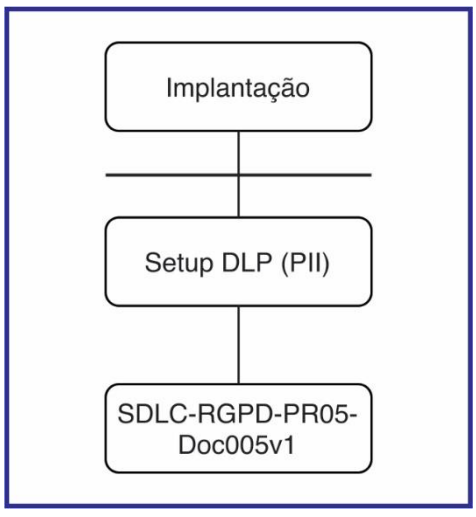


Figura 5.5.3 - Atividade solução data loss prevention

O conjunto de atividades do procedimento da fase SLDC implantação é apresentado na Figura 5.5.4. De seguida, apresentamos os documentos que detalham cada atividade dessa fase. Nessa penúltima fase do SDLC a equipa de produção é responsável pelo preenchimento dos documentos para ficar salvaguardado a maior conformidade da aplicação desenvolvida com as abordagens exigidas pelo RGPD.

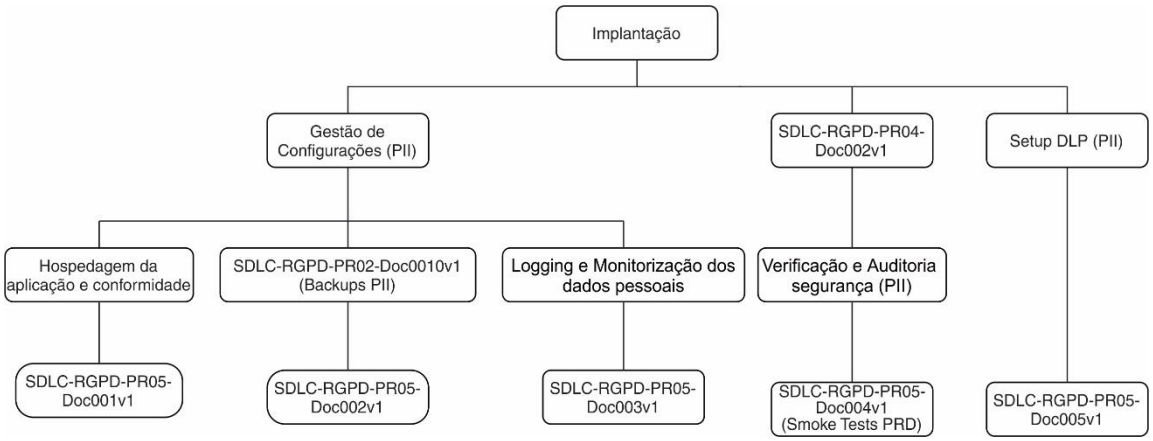


Figura 5.5.4 - Conjunto de atividades do procedimento Implantação

O primeiro documento a ser preenchido na implantação, tal como ilustrado na Figura 5.5.5, denomina-se Alojamento da Aplicação (Binários) e (*Storage*) – documento SDLC-RGPD-PR05-Doc001v1. O documento começa por registar o tipo de hospedagem da aplicação, se será interno ou externo. Em seguida o tipo de alojamento que ela terá com algumas opções, como por exemplo servidor dedicado, servidor partilhado, *cloud* privada ou outro tipo. Também aborda a consola de gestão, para definir o tipo de acesso (interno, externo ou outro). De seguida são registados aspetos relativos ao *storage*, sendo exemplificados tipos de *storage* para assinalar o utilizado.

ALOJAMENTO APLICAÇÃO (Binários)

Hospedagem	Tipo alojamento	Consola de Gestão	Conformidade RGPD
Interno ☐	Servidor Dedicado ☐ Servidor Partilhado ☐ Cloud Privada ☐ Outro ☐ _____	Acesso Pessoal Interno ☐ Acesso Pessoal Externo ☐ Outro ☐ _____	Sim ☐ Não ☐ N.A. ☐
Externo ☐	Servidor Dedicado ☐ Servidor Partilhado ☐ Cloud Privada ☐ Cloud Pública ☐ Outro ☐ _____	Acesso Pessoal Interno ☐ Acesso Pessoal Externo ☐ Outro ☐ _____	Sim ☐ Não ☐ N.A. ☐
Obs:			

ALOJAMENTO DADOS APLICAÇÃO (Storage)

Storage	Tipo storage	Consola de Gestão	Conformidade RGPD
Interno ☐	Dedicado ☐ Partilhado ☐ Em conjunto com a aplicação ☐ Cifrado ☐ Outro ☐ _____	Pessoal Interno ☐ Pessoal Externo ☐ Outro ☐ _____	Sim ☐ Não ☐ N.A. ☐
Externo ☐	Dedicado ☐ Partilhado ☐ Em conjunto com a aplicação ☐ Cifrado ☐ Outro ☐ _____	Pessoal Interno ☐ Pessoal Externo ☐ Outro ☐ _____	Sim ☐ Não ☐ N.A. ☐
Obs:			

Figura 5.5.5 - Documento Alojamento da Aplicação

Outro documento com grande importância nessa fase é o dos Backups Dados Pessoais - SDLC-RGPD-PR05-Doc002v1- ilustrado na Figura 5.5.6. Neste documento é preenchido o backup adotado para a aplicação (interno ou interno) e o tipo de backups (*online*, *offline* ou outro). É igualmente registado se a reposição dos *backups* foi testada e se o plano corresponde ao plano de *backup* definido na fase de desenho.

BACKUPS DADOS PESSOAIS

Backups	Tipo de backups	Backup e Reposição Testados	Implementado de acordo com o plano
Interno ☐	Online ☐ Offline ☐ Outro ☐ _____	Sim ☐ Não ☐	Sim ☐ Não ☐
Externo ☐	Online ☐ Offline ☐ Outro ☐ _____	Sim ☐ Não ☐	Sim ☐ Não ☐
Obs:			

Figura 5.5.6 - Documento Backups Dados Pessoais SDLC implantação

O próximo documento é ilustrado na Figura 5.5.7. Designa-se por *Logging* e Monitorização dos Dados Pessoais - SDLC-RGPD-PR05-Doc003v1 e começa por anotar se o controlo de acesso a aplicação foi registado em *log*, caso afirmativo, apresentar o formato (exemplo). Dando continuidade, verifica se há alguma monitorização sobre esse *log* de alerta e qual o destino desse alerta. Posteriormente aborda sobre o acesso (ler, alterar e remover) de dados pessoais, se foi registado em *log* cada ação e qual o formato (exemplo) do *log*. Também regista a existência ou não de monitorização sobre o acesso aos dados pessoais e qual o alerta gerado bem como o destino dado a esse alerta. O mesmo registo é feito sobre os direitos exercidos pelos titulares dos dados.

LOGGING E MONITORIZAÇÃO DE DADOS PESSOAIS

Controlo de acessos registado em log: Sim ☐ Não ☐

Log e formato (exemplo):

Existe monitorização sobre o log de controlo de acessos: Sim ☐ Não ☐

Alerta e destino:

Acesso (ler, alterar, remover) aos dados pessoais registado em log: Sim ☐ Não ☐

Log e formato (exemplo):

Existe monitorização sobre o acesso aos dados pessoais: Sim ☐ Não ☐

Alerta e destino:

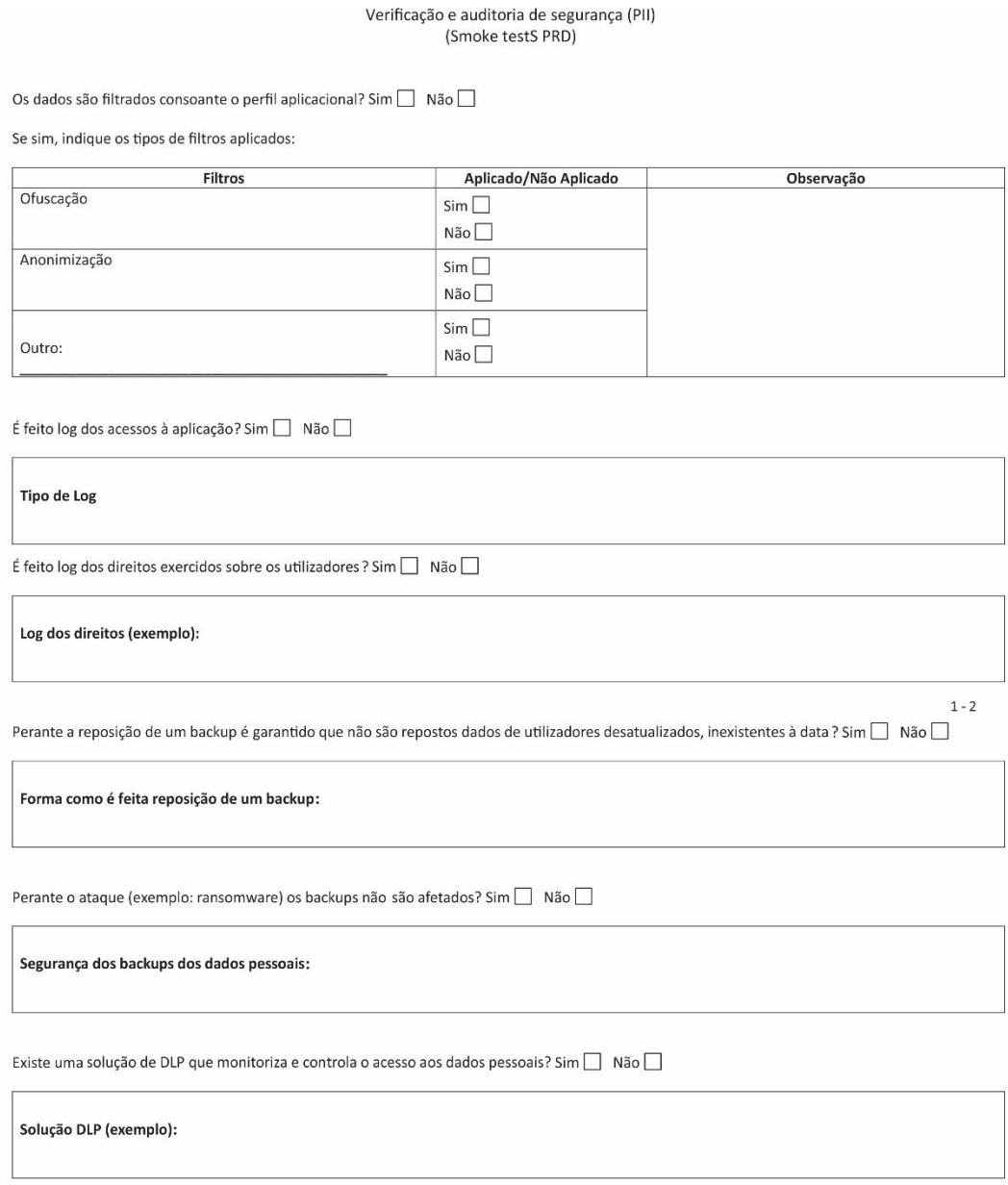
Direitos exercidos pelos utilizadores guardados em log: Sim ☐ Não ☐

Acesso	**Log e formato (exemplo):**
Esquecimento	**Log e formato (exemplo):**
Atualização	**Log e formato (exemplo):**
Portabilidade	**Log e formato (exemplo):**
Outro: _____ _____	**Log e formato (exemplo):**

Figura 5.5.7 - Documento Logging e Monitorização de Dados Pessoais

Ainda no âmbito do procedimento, foi criado o documento Verificação e Auditoria de Segurança (PII) (Smoke tests PRD) - SDLC-RGPD-PR05-Doc004v1. A primeira parte do documento é ilustrado na Figura 5.5.8, e tem por objetivo registar se os dados são filtrados consoante ao perfil aplicacional que os acede. Se afirmativo, deve ser indicado o tipo de filtro utilizado (ofuscação, anonimização ou outro). Ademais, questiona se é feito o log de acessos à aplicação por forma a dispor de evidências sobre os acessos. O documento regista ainda se na reposição de backup não estão a ser repostos dados desatualizados, ou seja, repostos por exemplos dados relativos a titulares que já exerceram um pedido de esquecimento. Ainda sobre os backups, interroga se, por exemplo numa situação de ataque como um *ransomware* os dados pessoais estão salvaguardados, ou seja, não são afetados pelo ataque. Por fim,

indaga se na aplicação foi inserida alguma solução DLP para monitorizar e controlar o acesso aos dados, apresentando um exemplo.



Verificação e auditoria de segurança (PII)
(Smoke testS PRD)

Os dados são filtrados consoante o perfil aplicacional? Sim ☐ Não ☐

Se sim, indique os tipos de filtros aplicados:

Filtros	Aplicado/Não Aplicado	Observação
Ofuscação	Sim ☐ Não ☐	
Anonimização	Sim ☐ Não ☐	
Outro: _____	Sim ☐ Não ☐	

É feito log dos acessos à aplicação? Sim ☐ Não ☐

Tipo de Log

É feito log dos direitos exercidos sobre os utilizadores ? Sim ☐ Não ☐

Log dos direitos (exemplo):

1 - 2

Perante a reposição de um backup é garantido que não são repostos dados de utilizadores desatualizados, inexistentes à data ? Sim ☐ Não ☐

Forma como é feita reposição de um backup:

Perante o ataque (exemplo: ransomware) os backups não são afetados? Sim ☐ Não ☐

Segurança dos backups dos dados pessoais:

Existe uma solução de DLP que monitoriza e controla o acesso aos dados pessoais? Sim ☐ Não ☐

Solução DLP (exemplo):

Figura 5.5.8 - Documento Verificação e auditoria de segurança (PII) (Smoke tests PRD)

O último documento criado referente ao SDLC implantação, tal como ilustrado na Figura 5.5.9, é referente a Solução Data Loss Prevention – documento SDLC-RGPD-PR05-Doc005v1. O objetivo dele é inicialmente, registar se existe alguma solução DLP associada à aplicação. Caso positivo, deve-se assinalar os controlos ativos com relação aos dados pessoais e sensíveis. A seguir, é questionado sobre o tipo de monitorização cobertos pela solução, apresentando alguns tipos de monitorização comuns como, *Data at rest*, *Data in use*, *Data in motion* e Monitorização ativa de *Data Leaks*, com os destaques das explicações dos controlos ativados.

SOLUÇÃO DATA LOSS PREVENTION

Existe alguma solução de DLP afeta à aplicação: Sim ☐ Não ☐

Se sim, indique quais dos controlos foram ativados relativamente à aplicação:

Controlo	Ativado?
Identificação de dados pessoais/sensíveis	Sim ☐ Não ☐
Classificação dos dados pessoais/sensíveis	Sim ☐ Não ☐
Monitorização das atividades que envolvem os dados pessoais/sensíveis	Sim ☐ Não ☐

Indique os tipos de monitorização cobertos pela solução de DLP:

Tipo monitorização	Controlos ativados
Data at rest	Restringir o acesso às funções administrativas locais, como a capacidade de instalar o software e modificar as configurações de segurança. Impedir malware, vírus, spyware, etc. Impedir a cópia de dados confidenciais em mídia não aprovada. Verificar se a extração autorizada de dados ocorre apenas na mídia criptografada.
Data in use	Monitorizar o acesso e o uso de dados de alto risco para identificar o uso potencialmente inadequado. Restringir as habilidades do usuário para copiar dados confidenciais em contêineres não aprovados (por exemplo, email, navegadores da Web), incluindo o controle da capacidade de copiar, colar e imprimir seções de documentos.
Data in motion	Impedir que dados confidenciais não criptografados deixem o perímetro. Registrar e monitorizar o tráfego de rede para identificar e investigar transferências inadequadas de dados sensíveis.

Figura 5.5.9 - Documento Solução Data Loss Prevention

5.6. Fase de Manutenção – SDLC e RGPD

A última fase do SDLC manutenção, inicia o procedimento com uma atividade que consiste em verificar se houve melhoria ou atualização do software com impacto na forma como são feitos os backups. A atividade é ilustrada na Figura 5.6.1. Caso a aplicação não tenha sofrido nenhuma mudança, a atividade finaliza. Senão, segue para condição de verificar se essa melhoria teve impacto no backup dos dados pessoais. Em caso negativo finaliza a atividade, em caso positivo o impacto é registado no documento Alteração nos backups - SDLC-RGPD-PR06-Doc001v1.

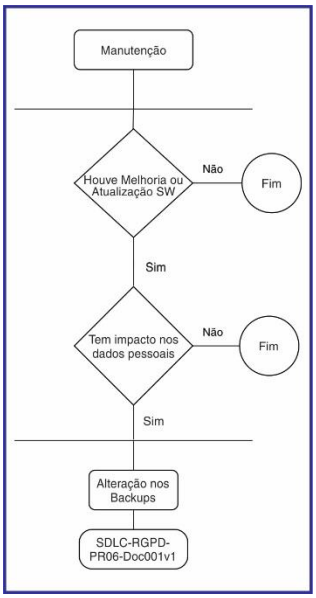


Figura 5.6.1 - Atividade manutenção alteração nos backups

As outras atividades da fase manutenção seguem essa mesma estrutura da apresentada anteriormente. Sempre que forem confirmadas alterações que envolvam dados pessoais, faz-se o registo das mesmas nos documentos. Por isso verifica-se se houve alterações na Matriz de Acesso - SDLC-RGPD-PR06-Doc002v1- alterações nos direitos dos titulares dos dados - SDLC-RGPD-PR06-Doc003v1 - ou outro tipo de alterações merecedoras de registo - SDLC-RGPD-PR06-Doc004v1. O conjunto das atividades do procedimento da fase SDLC manutenção alinhada com o RGPD é ilustrado na Figura 5.6.2.

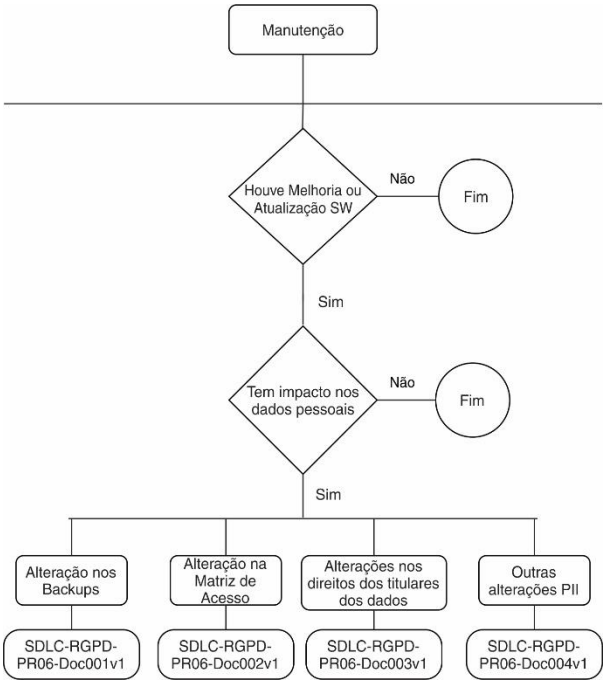


Figura 5.6.2 - Conjunto de atividades do procedimento Manutenção

Em relação aos documentos dessa fase, o primeiro como indicado na Figura 5.6.3, Alteração nos Backups dos Dados Pessoais – Data at Rest - SDLC-RGPD-PR06-Doc001v1 - verifica se houve alguma alteração na informação que foi recolhida da fase de análise e especificação de requisitos com relação aos backups que afeta a salvaguarda dos dados pessoais. Caso tenha ocorrido, recomenda-se descrever a alteração do plano de backups em relação ao tipo, periodicidade, segurança e local alterados com as observações referente às mudanças. Esse documento deverá constar a data e o nome do responsável por essa manutenção.

ALTERAÇÃO NOS BACKUPS DOS DADOS PESSOAIS – DATA AT REST

1 – Alteração na informação recolhida da fase de análise e especificação de requisitos

Houve alterações nos backups que afetam a salvaguarda de dados pessoais: Sim ☐ Não ☐

Se SIM descreva alteração do plano de backups:

Tipo	Periodicidade	Tipo	Segurança	Local
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Outro		Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐

Observações referente às alterações:

Data: ___ / ___ /_____ Nome: _____

Figura 5.6.3 - Documento Alteração nos Backups dos Dados Pessoais – Data At Rest

O segundo documento da manutenção, tal como ilustrado na Figura 5.6.4, designa-se por Alteração na Matriz de Acessos (Data Mapping) - SDLC-RGPD-PR06-Doc002v1 - e regista eventuais alterações na matriz de acesso. Caso afirmativo, devem ser descritas às alterações, especificando o utilizador ou perfil com o campo que sofreu a modificação. Nesse documento, só devem ser registados alterações e no final constar a data e o nome do responsável pela realização.

ALTERAÇÃO NA MATRIZ DE ACESSOS / DADOS (DATA MAPPING)

Houve alterações nos backups que afetam a salvaguarda de dados pessoais: Sim ( ) Não ( )

Se SIM descreva alteração do plano de backups:

Data da alteração: ___/ ___/____ **Nome:**

INSTRUÇÕES: **SÓ DEVEM SER REGISTADAS AS ALTERAÇÕES!**
Especificar os campos da BD relativos às **alterações** dos dados pessoais/sensíveis na linha 6
Especificar **alterações** dos utilizadores/perfis na coluna A

Completar com S/N sendo "S" da **alteração** na indicação de operação permitida sobre os campos pelo utilizador/perfil e "N" a indicação de acesso proibido/desnecessário do utilizador/perfil correspondente

Função / Campo e Operações	Primeiro Nome				Sobrenome				Último nome				Telefone				Morada				Emi	
	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R
admin		S		S				S				S		S		S				S		S
rh				S				S				S				S				S		
inf				S				N				N				N				N		
ana@xpto.com				N				N				N				N				N		
manuel@xpto.com				S				N				N				S				N		
DPO				S				S				S				S				N		
...				S				S				S				S				S		
...																						

Figura 5.6.4 - Documento Alteração na Matriz de Acessos / Dados (Data Mapping

Outro documento de suporte a esta fase do SDLC é ilustrado na Figura 5.6.5, denomina-se Alteração Direitos dos Utilizadores - SDLC-RGPD-PR06-Doc003v1 - e foi criado para registar quais direitos foram alterados na fase de manutenção. Todas as vezes que ocorrer alguma mudança desses critérios, deve-se guardar as modificações com a data e o nome da pessoa que realizou o procedimento.

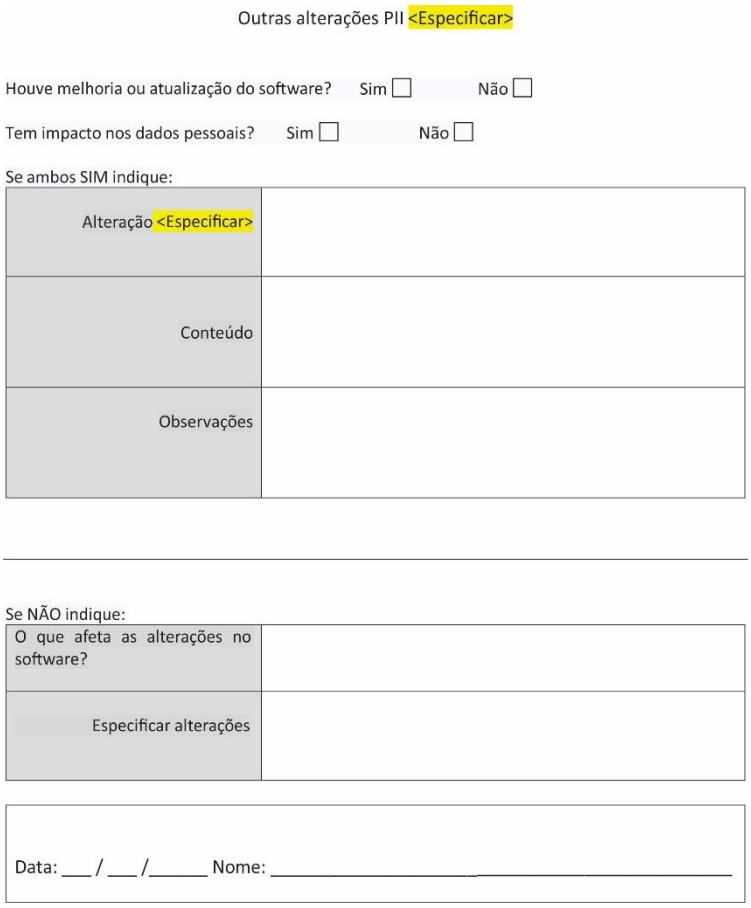
ALTERAÇÃO DIREITOS DOS UTILIZADORES

Direito	Alterado	Formato	Observações das alterações
Acesso	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Portabilidade	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Esquecimento	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Atualização	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	

Data: ___ / ___ /_____ Nome: _____

Figura 5.6.5 - Documento Alteração Direitos dos Utilizadores

O último documento do procedimento é ilustrado na Figura 5.6.6. Trata-se do documento de registo de Outras alterações PII - SDLC-RGPD-PR06-Doc004v1. Caso tenha ocorrido alguma melhoria ou atualização do software e elas tiveram impacto nos dados pessoais do projeto, então recomenda-se registar a alteração, o conteúdo e as observações dessas mudanças. Perante alterações que não afetam dados pessoais, deve-se registar apenas as que afetam, facilitando o acompanhamento temporal das mudanças na aplicação.



Outras alterações PII <Especificar>

Houve melhoria ou atualização do software? Sim ☐ Não ☐

Tem impacto nos dados pessoais? Sim ☐ Não ☐

Se ambos SIM indique:

Alteração <Especificar>	
Conteúdo	
Observações	

Se NÃO indique:

O que afeta as alterações no software?	
Especificar alterações	

Data: ___ / ___ /_____ Nome: _____

Figura 5.6.6 - Documento Outras Alterações PII

Os procedimentos apresentados ao longo do capítulo divide-se em seis fases, cada uma com as atividades correspondentes a fase do SDLC. Por si, cada procedimento contém diversas atividades que visam recolher e registar informação que vai de encontro a uma implementação de software mais alinhada com o RGPD. À primeira vista pode parecer que se introduz complexidade e burocracia, no entanto e tal como acontece noutros procedimentos (por exemplo, num sistema de gestão da qualidade) a utilização torna-se benéfica, porque padroniza a forma de trabalhar e formalizar um conjunto de etapas que resultam no projeto de maior qualidade e consequentemente na proteção contra ataques à informação pessoal, ou na apresentação clara e evidente de boas práticas no sentido dessa proteção às entidades reguladoras.

Capítulo 6

Conclusão

Neste capítulo é apresentado um resumo de trabalho desenvolvido e as principais conclusões. Também é mencionado trabalho futuro que irá contribuir para a melhoria da ferramenta proposta.

6.1 Trabalho realizado e conclusão

Nesta proposta apresentamos um processo de referência para alinhar o ciclo de desenvolvimento de software com o RGPD numa perspetiva prática de adoção de controlos ao longo do ciclo de desenvolvimento que visam melhorar a segurança dos dados pessoais. Na base do processo foram analisadas normas (e.g.: ISO 27018, 29100, 29134, 29151) que de alguma forma focam a proteção de dados pessoais, e foi também considerado o RGPD. O resultado é um processo, dividido em vários procedimentos, um por fase do SDLC, enquadrando o ciclo de desenvolvimento do software e incorporando princípios e meios para alcançar aplicações informáticas seguras por defeito e por padrão de acordo com os artigos 5º e 25º do RGPD.

Como ferramenta de suporte à criação do processo, foi efetuado um inquérito dirigido a equipas de desenvolvimento de DPO. As questões e respostas focaram sobretudo questões relacionadas com as práticas aplicadas ao ciclo de desenvolvimento de software relativas à proteção de dados pessoais. Os resultados obtidos permitem verificar que a maioria das organizações está preocupada com o problema, que uma parte delas já realiza tarefas que visam dotar o software de controlos de segurança sobre os dados pessoais. Porém, muitas ainda desconhecem ou não aplicam qualquer prática a esse respeito.

A disponibilização de um processo, como o que foi apresentado neste relatório, permite às equipas de desenvolvimento recolher requisitos, desenhar interfaces e modelos, implementar controlos de acesso granulares, especificar backups que tenham em consideração questões específicas introduzidas pelo RGPD, entre outros. Ainda que aparentemente pareça ser um processo burocrático, o mesmo foi apresentado na entidade de acolhimento e a informação obtida é que o processo deverá ser testado e avaliado, mas que se perspetiva que o mesmo permite aos envolvidos no ciclo de desenvolvimento ter em consideração os aspetos de segurança desde cedo, o que resultará com certeza num produto final mais alinhado com o propósito do RGPD. Da mesma forma as organizações ficam mais seguras dos seus procedimentos e protegidas contra eventuais situações de perda de dados e penalizações que decorrem dessa perda. As equipas envolvidas no SDLC ficarão também mais suportadas com a definição clara de tarefas e ações a executar em cada uma das fases.

É de esperar que o processo venha a ser revisto, mediante a sua aplicação prática e avaliação do mesmo. Em todo o caso, consideramos a existência do mesmo uma mais valia para as organizações.

6.2 Trabalho futuro

Em relação ao trabalho futuro a ser desenvolvido, será inicialmente aplicá-lo ao próximo projeto da empresa onde estou estagiando nas fases do SDLC com a equipa que faço parte de desenvolvimento. Em seguida disponibilizar também essa ferramenta para outras organizações passarem a adotar o processo nas aplicações que terão dados pessoais.

Outro passo será desenvolver uma aplicação informática de suporte ao processo, criando desse modo um sistema para guardar as informações também de forma digital.

Tal aplicação terá todas as fases do SDLC e contará com o registo de acesso de cada responsável por cada etapa que ele está envolvido. Por exemplo, o analista acederá a janela referente às suas atribuições e poderá visualizar o procedimento e atividades dessa fase e preencherá os documentos que estarão lá disponíveis. Em seguida o DPO e o gestor do projeto poderão também verificar os relatórios e documentar com uma assinatura digital.

Posteriormente o desenhista com as suas credenciais de acesso, poderá ver os documentos da fase anterior, em seguida o procedimento com as atividades e os documentos para fazer a parte do seu trabalho, gerando o documento também o documento final de especificação para a fase seguinte contendo as assinaturas do DPO e gestor. O desenvolvedor com os seus dados de acesso entrará na aplicação e poderá visualizar os arquivos da fase desenho para iniciar a codificação da aplicação de acordo com o procedimento e as atividades dessa fase, com as orientações e recomendações referentes aos documentos anteriores.

No final também preencherá os documentos a respeito da criação da aplicação para auxiliar nas fases seguintes. Esses passos se repetirão para as equipas de teste, implantação do sistema e a manutenção, sendo que, em todas as fases serão acompanhadas pelo visto do DPO e gestor do projeto. Todos envolvidos deverão ter acesso a essa aplicação para terem essa ferramenta para ajudar durante todas as fases do desenvolvimento. Com a criação dessa aplicação e colocados os procedimentos com o conjunto de atividades e documentos criados nela as organizações terão duas formas de arquivar os documentos, a primeira em arquivo de papel e a outra em arquivo digital.

Essa aplicação ficará disponível para as empresas interessadas em adotar essa metodologia e incluir no desenvolvimento, com o objetivo de salvaguardar os dados pessoais dos titulares das informações pessoais, a maior conformidade com às exigências e orientações do RGPD.

Bibliografia

[1] P. MENDES, “Análise de Risco no GDPR,” pp. 20-21, 2018. Accessed on: Sept. 9, 2020. [Online]. Available: http://hdl.handle.net/10451/35494

[2] European Data Protection Supervisor, *Preliminary Opinion on privacy by design*, May 31, 2018. Accessed on: Sept. 1, 2020. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

[3] N. Vollmer, 2018, *Artigo 25 UE Regulamento Geral sobre a Proteção de Dados "- Proteção de dados desde a conceção e por defeito"*. Accessed on: Aug. 20, 2020. [Online]. Available: https://www.privacy-regulation.eu/pt/25.htm

[4] T. Figueiredo, “Da Responsabilidade do Subcontratante no Âmbito do RGPD”, pp. 13-24, 2019. Accessed on: Aug. 8, 2020. [Online]. Available: https://repositorio.ucp.pt/bitstream/10400.14/28688/1/TomasFigueiredo_Da%20Responsabilidade%20do%20Subcontratante%20no%20%C3%A2mbito%20do%20RGPD.pdf

[5] J._Ilic, *Top 10 GDPR Breaches in 2019 Cause €402.6 Million Fines*, Precise Security, Feb. 19, 2020. Accessed on: Aug. 21, 2020. [Online]. Available: https://www.precisesecurity.com/articles/top-10-gdpr-breaches-in-2019-cause-e402-6-million-fines/

[6] It Insight, *RGPD: S21Sec partilha medidas para uma compliance à prova de tudo*, It Insight, Apr. 2018, Accessed: Aug. 21, 2020. [Online]. Available: https://www.itinsight.pt/news/seguranca/rgpd-s21sec-partilha-medidas-para-uma-compliance-a-prova-de-tudo

[7] Nymity Innovating Compliance, *Framework for Demonstrable GDPR Compliance*, Dec. 2,2018. Accessed: Jul. 19, 2020. [Online]. Available: https://iapp.org/media/pdf/resource_center/Nymit-Accountability-Roadmap-GDPR-Compliance.pdf

[8] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*, May 2019, Accessed: Aug. 8, 2020. [Online]. Available: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

[9] A. Cavoukian, “Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices,” *Inf. Priv. Comm. Ontario, Canada*, pp. 2-5, Oct. 2017. Accessed: Aug. 5, 2020. [Online]. Available: http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf

[10] UNCTAD, *Data Protection and Privacy Legislation Worldwide*, Sep. 21, 2020. Accessed: Aug. 21, 2020. [Online]. Available: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[11] G. Greenleaf, “Global data privacy laws 2019: 132 national laws and many bills,” *SSRN Electron. J.*, pp. 1-4, May 2019. Accessed: Aug. 21, 2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593

[12] D. Cohen, *HIPAA Reform or a Patchwork Scheme : A Look at Preemption , Scope , and the Inclusion of a Private Right of Action in a New Federal Data Privacy Law*, Digital Commons @ American University Washington College of Law, 2020. Accessed: Aug. 18, 2020. [Online]. Available:https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1040&context=stu_upperlevel_papers

[13] G. Silva, “RGPD aplicado nas PME portuguesas”, *Repositório Universidade Nova*, pp. 10-23, Feb. 4, 2020. Accessed: Aug. 8, 2020. [Online]. Available: https://run.unl.pt/handle/10362/94888

[14] M. Miri, F. Foomany, and N. Mohammed, “Complying With GDPR,” *Isaca*, vol. 2, pp. 1–7, 2018.

[15] A. Silveira, J. Abreu, and L. Coelho, *UNIO Ebook Interop 2019: O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir*. 2019, Repositório Universidade do Minho, Jul. 2019. Accessed: Aug. 9, 2020. [Online]. Available: http://repositorium.sdum.uminho.pt/handle/1822/61446

[16] N. Vollmer, *Artigo 32 UE Regulamento Geral sobre a Proteção de Dados "- Segurança do tratamento"*, Privacy Regulation, May 2020. Accessed: Aug. 10, 2020. [Online]. Available: https://www.privacy-regulation.eu/pt/32.htm

[17] N. Vollmer, *Artigo 5 UE Regulamento Geral sobre a Proteção de Dados "- Princípios relativos ao tratamento de dados pessoais"*, Privacy Regulation, May 2020. Accessed: Aug. 10, 2020 [Online]. Available: https://www.privacy-regulation.eu/pt/5.htm

[18] M. Mahmood, “System Development Methods — A Comparative Investigation”, *JSTOR*, vol. 11, no. 3, pp. 293-311, Sept. 1987.

[19] B. Sahil, S. Ankur, and U. Rani, “A detailed study of Software Development Life Cycle (SDLC) Models,” *Bull. Soc. Pathol. Exot.*, vol. 91, no. 1, pp. 1-4, 2017.

[20] J. Fernandes, and R. Machado, *Requisitos em projetos de software e de sistemas de informação*., Books google, Mar. 2018. Accessed: Aug. 10, 2020 [Online]. Available: https://www.google.com/search?tbm=bks&q=Requisitos+em+projetos+de+software+e+de+sistemas+de+informa%C3%A7%C3%A3o

[21] M. Oliveira, “Privacidade no Ciclo de Vida do Desenvolvimento Seguro”, pp. 23-89, 2019. Accessed on: Aug. 9, 2020. [Online]. Available: https://repositorio.ul.pt/bitstream/10451/40204/1/ulfc125562_tm_Manuel_Oliveira.pdf

[22] V. Igorevich, “Critical data leak detection in institutions”, pp. 17-24, 2019. Accessed on: Aug. 30, 2020. [Online]. Available: https://bibliotecadigital.ipb.pt/handle/10198/22691

[23] J. Hoepman, “Privacy Design Strategies,” pp. 446–459, 2014.

[24] Openlimits, *RGPD - Glossário: Todos os termos que precisa de conhecer,* Openlimits, Jul. 11, 2017. Accessed on: Sept. 11, 2020. [Online]. Available: https://www.openlimits.pt/pt/thinking-ahead-blog/glossario-rgpd-regulamento-europeu-protecao-dados/?all=1

[25] International Standard Organization, *ISO/IEC 29100 Information technology — Security techniques — Privacy framework*, ISO, Dec. 15, 2011. Accessed on: Jul. 11, 2020. [Online]. Available: https://www.iso.org/standard/45123.html

[26] J. Azevedo, "Análise de Segurança e Aperfeiçoamento de uma Rede Universitária de Telecomunicações", pp. 16-22, 2019. Accessed on: Sept. 12, 2020. [Online]. Available: https://digituma.uma.pt/bitstream/10400.13/2342/1/MestradoJoaoAzevedo.pdf

[27] M. Muller, *Quais são e para quê servem as normas de segurança da informação?*, Any Consulting, Mar. 30, 2017. Accessed on: Sept. 5, 2020. [Online]. Available: https://www.anyconsulting.com.br/normas-de-seguranca-da-informacao/

[28] C. Araujo, "Computação em nuvem: um estudo sobre a distribuição da produção de artigos publicados no período de 2007 a 2016", pp. 18, 2018. Accessed on: Sept. 6, 2020. [Online]. Available: https://bdm.unb.br/handle/10483/18934

[29] International Standard Organization, *ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*, ISO, Jan. 10, 2019. Accessed on: Jul. 11, 2020. [Online]. Available: https://www.iso.org/standard/76559.html

[30] International Standard, *ISO/IEC 29151 Information t echnology — Security techniques — Code of practice for personally identifiable information protection*, ISO, Aug. 2017. Accessed on: Jul. 09, 2020. [Online]. Available: https://www.iso.org/standard/62726.html

[31] C. Silva, *Tag Archives: RGPD; Artigo 42; ISO; 27001; 27002; 29151; 27552; Privacy ; SGPD; Privacidade; Proteção de Dados; Sistema; Conformidade; Compliance*, Control Gal, Jan. 4, 2019. Accessed on: Jul. 20, 2020. [Online]. Available: https://www.controlgal.pt/tag/rgpdartigo-42iso-27001-27002-2915127552privacysgpdprivacidadeprotecao-de-dadossistemaconformidadecompliance/

[32] International Standard, *ISO / IEC 29134 Information technology — Security techniques — Guidelines for privacy impact assessment*, ISO, June 2017. Accessed on: Jul. 13, 2020. [Online]. Available: https://www.iso.org/standard/62289.html

[33] E. Oliveira, *MIC- Metodologias de Investigação Científica MIC- Metodologias de Investigação Científica*, 2017. Accessed on: Jul. 5, 2020. [Online]. Available: https://paginas.fe.up.pt/~eol/PRODEI/mic1415_files/Teorias.pdf

ANEXO A – Inquérito SDLC RGPD

Inquérito para DPO e Equipas de Desenvolvimento

Survey SDLC RGPD
1.From 1 to 5 indicate (1 being minor and 5 very important) As a DPO, indicate the importance of carrying out an impact assessment on the protection of personal data:
1
2
3
4
5
2. In your organization/team, is there a known formal process that facilitates the adoption of the GDPR principles during the software development process?
Yes
No
3. According to your experience, does the DPO and the development team discuss in advance aspects related to the GDPR that are important for the design of the application?
Yes
No
No opinion
4.From 1 to 5 indicate (1 being minor and 5 very important) How important is to have the data mapping defined i.e. DB fields, user/role and CRUD action before implement the granular access control level in the application:
1
2
3
4
5
5. In a process of specification, design and implementation of an application framed with the GDPR, consent must meet several criteria. Indicate for each criterion what you have applied in recent software development projects.

Free	Consent cannot be conditioned, that is, if the client does not give Consent, he does not have access to a certain product or service. The Data Owner may refuse or withdraw Consent without being harmed. Consent must be as easy to withdraw as it is to give.	Adopted	Not Adopted	Partially Adopted	Does not apply

Informed	The Consent text must have a clear, simple and easily accessible language. The Data Subject must be informed about the Purposes for which the Treatment is intended and about the right to withdraw Consent at any time.	Adopted / Not Adopted / Partially Adopted / Does not apply
Specific	The data owner must be able to give a Consent for each Purpose of the Treatment (example: giving marketing authorization is different from giving marketing authorization to third parties).	Adopted / Not Adopted / Partially Adopted / Does not apply
Express	The consent must be a positive act (written statement - including in electronic form - or oral statement). Silence, pre-validated options or omission do not constitute a Consent.	Adopted / Not Adopted / Partially Adopted / Does not apply
Keep evidence	It should be possible to demonstrate that the Data Subject has given his / her Consent for the Treatment of his / her Personal Data, that is, it must be possible to register and prove the date / time when the Consent was obtained, the communication channel used and the version Consent.	Adopted / Not Adopted / Partially Adopted / Does not apply

6. In the latest software projects you developed, did you used any security controls to ensure that only authorized persons have access to personal data?

Obfuscation	Anonymization	Pseudonymization	Encryption	Other	None

7. In the latest software projects in which you have been involved, which of the above controls have been contemplated so that users can easily exercise rights over their personal data?

Right	Yes	No	Partially
Access			
Rectification			
Erasure			
Portability			
Forgetfulness			

8. Considering the last projects you were involved in, did the backup of the application and its database take into account the safeguarding and restoration of personal data (any specific treatment/concern)?

Yes
No
No opinion

9.From 1 to 5 indicate (1 being minor and 5 very important) Indicate from 1 to 5, How useful do you think there is a process that facilitates the design and conception of applications aligned with the GDPR?
1
2
3
4
5
10. According to your experience, whenever there is an update to the application, are the security team, the DPO and the development team involved to take care of aspects related with personal data protection?
Always
Never
Sometimes

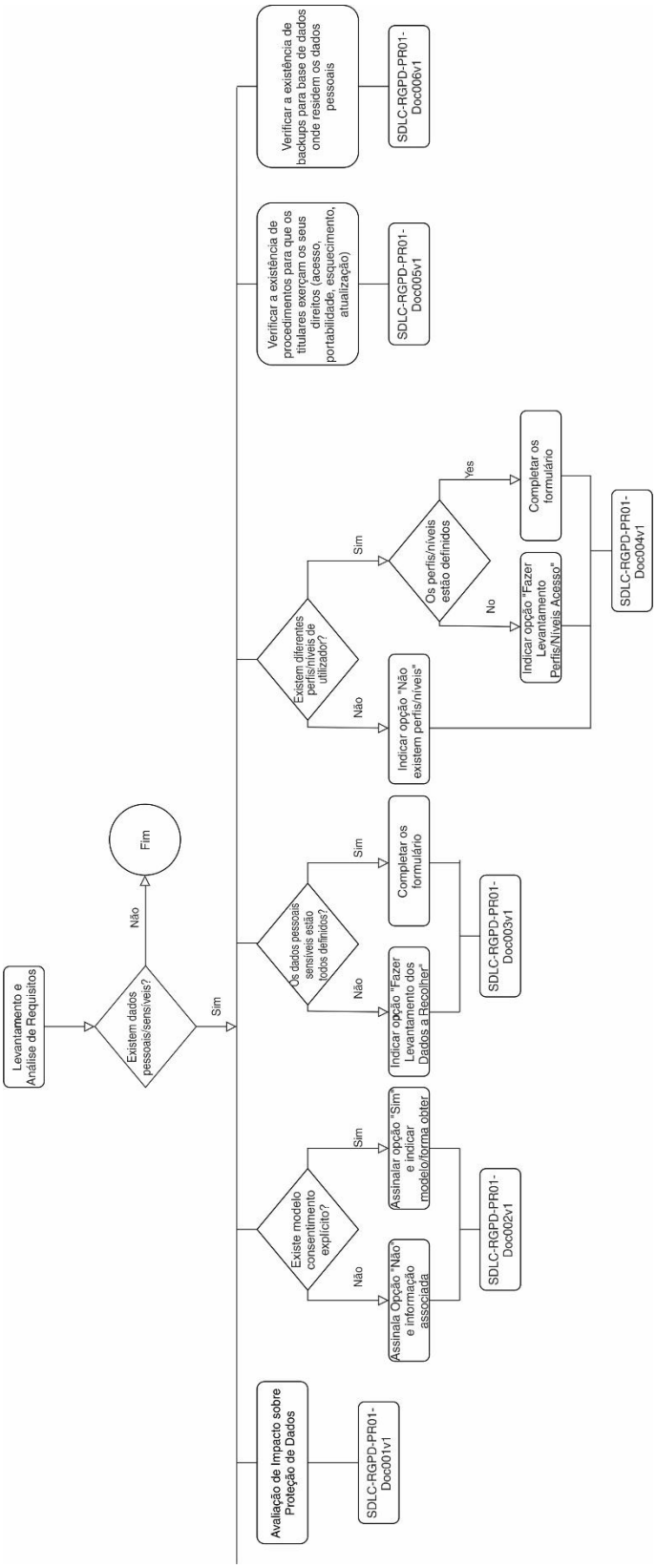
ANEXO B – Processo de alinhamento SDLC e RGPD (documentação)

O processo consta em documento a parte contemplando a versão portuguesa e a versão em inglês com o nome Processo SDLC RGPD com todos os procedimentos com as atividades e documentos desenvolvidos durante o projeto.

ANEXO B - PROCESSO PARA ALINHAMENTO SDLC E RGPD

Neste documento é apresentado o processo de alinhamento entre o SDLC e o RGPD. O processo é constituído por seis procedimentos. Para cada um dos procedimentos é apresentado as atividades com o fluxo de informação e documentos de suporte, o procedimento de cada fase separado fluxo a fluxo e com uma descrição para o tornar mais claro e ainda os modelos de cada documento de suporte.

Procedimento 1 - Análise de Requisitos



Documentos de Especificação Análise de Requisitos:

ESPECIFICAÇÃO DE REQUISITOS DE SEGURANÇA DE PII **SDLC-RGPD-PR01-Doc001v1**
FASE SDLC - ANÁLISE DE REQUISITOS

1. OBJETIVO E ÂMBITO

Documento questionário com objetivo de realizar a Avaliação de Impacto sobre a proteção dos dados pessoais / sensíveis.

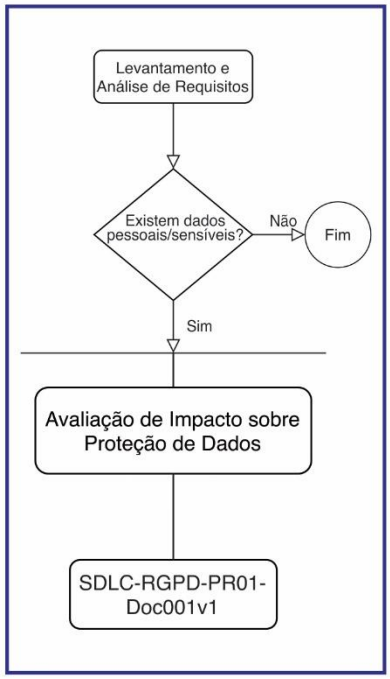
2. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

3. MODO DE PROCEDER

3.1 Documento de Requisitos: Doc001v1

3.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Realizar o levantamento e análise dos requisito e verificar se existirá dados pessoais / sensíveis na aplicação. Se não existir dados pessoais/sensíveis, é o Fim do processo. Se existir, realizar a avaliação de impacto sobre a proteção dos dados pessoais / sensíveis que a aplicação utilizará e determinar o âmbito, o objetivo, a equipe e responsáveis, as operações de tratamento dos dados pessoais, realizar todas as avaliações do documento e prever medidas de segurança com recomendações de melhorias.	Analista de Sistemas DPO	SDLC-RGPD-PR01-Doc.001V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

4. OBJETIVO E ÂMBITO

Questionário/entrevista para determinar se a aplicação faz uso de dados pessoais / sensíveis.
Verificar se existe modelo de consentimento explicito

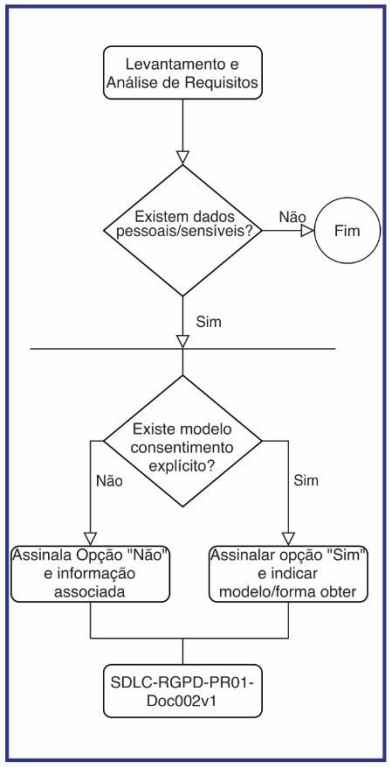
5. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

6. MODO DE PROCEDER

6.1 Documento de Requisitos: Doc002v1

6.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Este procedimento tem como objetivo a coleta de informações/especificação de requisitos das PII. Verificar se a aplicação faz uso de dados pessoais ou dados sensíveis que podem levar à identificação de uma determinada pessoa? - Primeiro Nome; - Último Nome; - Nome Completo; - Número de Telemóvel; - Número do CC; - Número do Passaporte; - Número de Identificação Fiscal; - Morada; - Estado Civil; etc. • Se não existir dados pessoais/sensíveis, é o fim do diagrama. • Se sim, continua a análise com a coleta dos outros requisitos abaixo. Existe algum modelo para pedido de consentimento explicito? • Se sim, fornecer o modelo indicado registando essa opção no documento CONSENTIMENTO. • Se não, verificar se o formulário de consentimento é adequado ao pedido ajustando o mesmo se necessário.	Analista de Sistemas Analista de Sistemas Analista de Sistemas Analista de Sistemas	SDLC-RGPD-PR01-Doc.002V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

7. OBJETIVO E ÂMBITO

Questionário/entrevista para determinar se os dados pessoais e sensíveis estão definidos e adequados ao projeto do software.

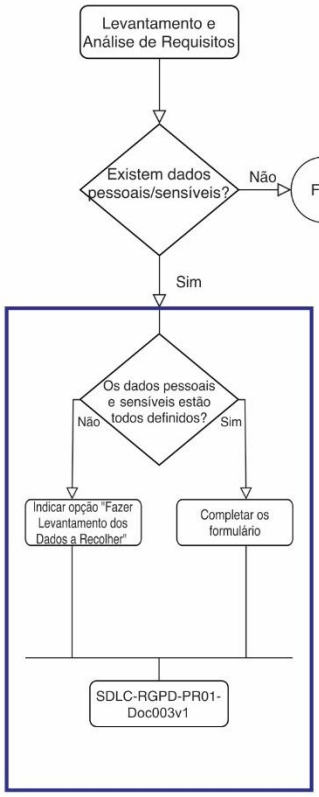
8. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

9. MODO DE PROCEDER

9.1 Documento de Requisitos: Doc003v1

9.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se o modelo para indicação dos dados pessoais e sensíveis a recolher e tratar é adequado ao projeto. • Se os dados já estiverem definidos, deverá preencher o Formulário DADOS-RECOLHER. • Se os dados pessoais a recolher não estiverem definidos, deverá fazer um levantamento para se proceder ao preenchimento do Formulário DADOS-RECOLHER.	Analista de Sistemas Analista de Sistemas Analista de Sistemas	SDLC-RGPD-PR01-Doc.003V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

10. OBJETIVO E ÂMBITO

Questionário/entrevista para verificar se existem níveis de acesso / perfis na aplicação

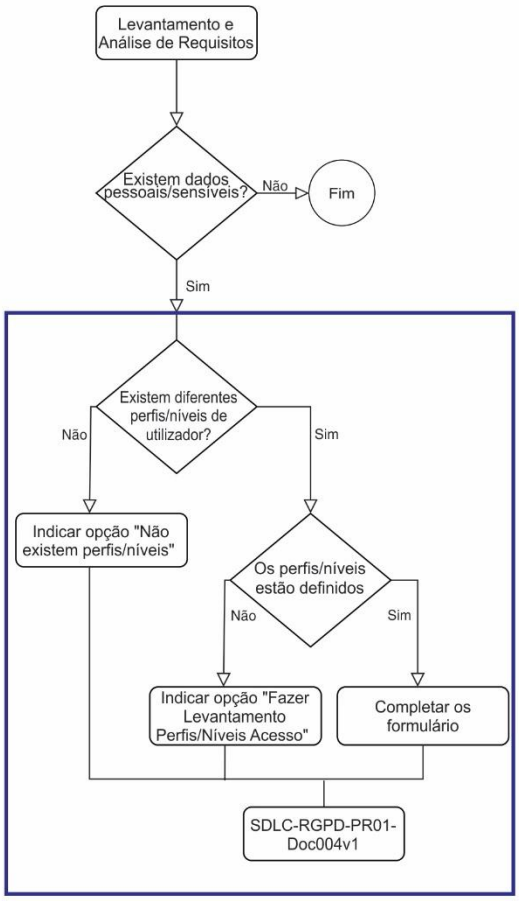
11. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

12. MODO DE PROCEDER

12.1 Documento de Requisitos: Doc004v1

12.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se existem níveis de acesso / perfis na aplicação. • Se não existirem níveis de acesso / perfis na aplicação, deverá indicar tal no documento PERFIS. • Se existirem níveis de acesso / perfis na aplicação, e se os mesmos já estiverem definidos então deve completar o documento PERFIS. • Se não estiverem definidos deverá fazer um levantamento para se proceder ao preenchimento do documento PERFIS.	Analista de Sistemas Analista de Sistemas Analista de Sistemas Analista de Sistemas	SDLC-RGPD-PR01-Doc.004V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

13. OBJETIVO E ÂMBITO

Questionário/entrevista para verificar a participação de acesso dos titulares dos dados pessoais sobre os seus direitos de acesso e pedidos.

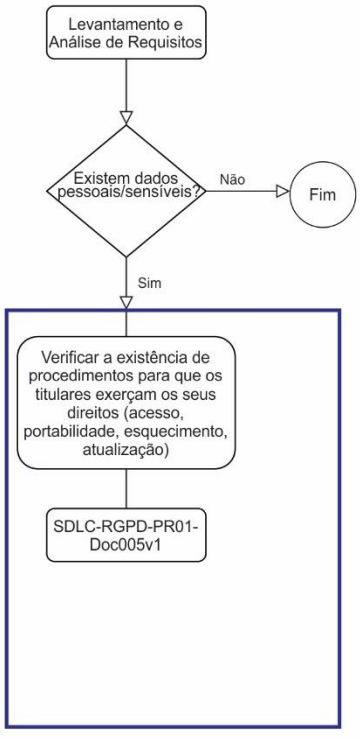
14. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

15. MODO DE PROCEDER

15.1 Documento de Requisitos: Doc005v1

15.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar como será a participação de acesso dos titulares dos dados pessoais relativamente aos seus direitos: • Direito de acesso aos dados pessoais; • Pedidos de portabilidade; • Pedidos de esquecimento dos dados pessoais; • Atualização dos dados pessoais. Registar as opções no formulário DIREITOS-TITULARES-DADOS.	Analista de Sistemas Analista de Sistemas	SDLC-RGPD-PR01-Doc.005V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

16. OBJETIVO E ÂMBITO

Questionário/entrevista para verificar se estão contemplados os backups da BD onde constam os dados pessoais para a aplicação.

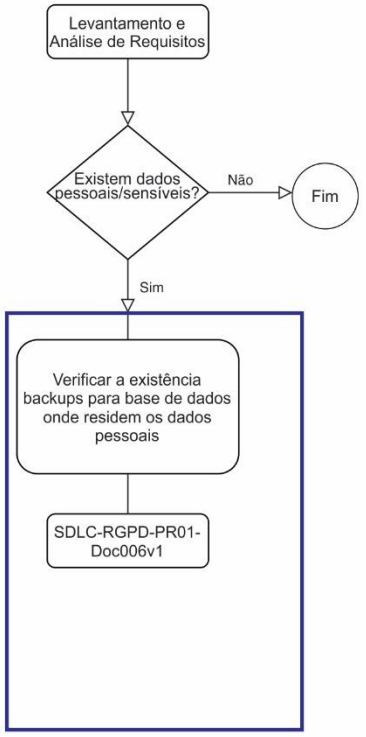
17. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1
BD - Base de Dados

18. MODO DE PROCEDER

18.1 Documento de Requisitos: Doc006v1

18.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se estão contemplados backups da BD onde constam os dados pessoais. • Se estiverem contemplados, o plano deve ser apresentado no documento BACKUPS. • Se não estiverem refletir a questão no documento BACKUPS com indicação do procedimento a adotar.	Analista de Sistemas Analista de Sistemas Analista de Sistemas	SDLC-RGPD-PR01-Doc.006V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

AVALIAÇÃO DE IMPACTO SOBRE PROTEÇÃO DE DADOS (AIPD)

1 - Âmbito da AIPD:

2 - Objetivo da avaliação de impacto

3 - Equipa e contactos dos responsáveis, indique:

Nome	Contato

---

4 - Operações de Tratamento de dados pessoais:

Contexto e finalidade do tratamento dos dados pessoais	
Ativos importantes que dependem de dados pessoais (componentes, sistemas, redes, papel)	
Acesso aos dados pessoais	<Será tratado pelo processo identificado no documento SDLC-RGPD-PR01-Doc004v1>
Descrição das operações de tratamento de dados pessoais	<Será tratado pelo processo identificado no documento SDLC-RGPD-PR01-Doc003v1>

---

5 - Avaliação das necessidades nas operações de processamento:

Medidas previstas para demonstrar a conformidade e necessidade do tratamento	

Medidas que contribuem para os direitos dos titulares dos dados	<Será tratado pelo processo identificado no documento SDLC-RGPD-PR01-Doc005v1>

---

6 - Avaliar e mitigar riscos inerentes do direito dos titulares dos dados:

Relacionados com a violação de confidencialidade ou integridade	
Relacionados com a perda de dados pessoais	
Relacionados com o exercício dos direitos dos titulares de dados	<Processo identificado no documento Direito dos utilizadores SDLC-RGPD-PR01-Doc005v1 >
Possíveis impactos e ameaças	
Medidas para redução dos riscos com descrições técnicas	

---

7 - Prever medidas de segurança e procedimentos para assegurar a proteção de dados:

Indique:

Descrição de medidas técnicas para assegurar a proteção	<Processo identificado no documento de Backups dos Dados Pessoais SDLC-RGPD-PR01-Doc006v1. Outras soluções técnicas constam nos documentos de manutenção SDLC-RGPD-PR05-Doc001v1, SDLC-RGPD-PR05-Doc002v1, SDLC-RGPD-PR05-Doc003v1, SDLC-RGPD-PR05-Doc004v1, SDLC-RGPD-PR05-Doc005v1>

8 - Recomendações de melhoria:

CONSENTIMENTO, PRIVACIDADE E TERMOS & CONDIÇÕES

Esta contemplado a salvaguarda do registo data/hora do consentimento, privacidade e termos & condições? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Existe modelo consentimento explícito? Sim ☐ Não ☐

Se SIM indique:

Como obter	
Pode ser usado sem adaptações	Sim ☐ Não ☐
Adaptações a fazer	

Se NÃO indique:

Delegar na fase de desenho	Sim ☐ Não ☐
Conteúdo	

Existe modelo política privacidade? Sim ☐ Não ☐

Se SIM indique:

Como obter	
Pode ser usado sem adaptações	Sim ☐ Não ☐
Adaptações a fazer	

Se NÃO indique:

Delegar na fase de desenho	Sim ☐ Não ☐
Conteúdo	

Existe modelo termos e condições? Sim ☐ Não ☐

Se SIM indique:

Como obter	
Pode ser usado sem adaptações	Sim ☐ Não ☐
Adaptações a fazer	

Se NÃO indique:

Delegar na fase de desenho	Sim ☐ Não ☐

Conteúdo	

RECOLHA E TRATAMENTO DE DADOS – ESPECIFICAÇÃO DE DADOS

Dados pessoais/sensíveis e recolher e tratar

Campo	Recolher S/N?	Justificação
Primeiro Nome	Sim ☐ Não ☐ a definir ☐	
Último Nome	Sim ☐ Não ☐ a definir ☐	
Nome completo	Sim ☐ Não ☐ a definir ☐	
Número de telemóvel	Sim ☐ Não ☐ a definir ☐	
Número do CC	Sim ☐ Não ☐ a definir ☐	
Número do passaporte	Sim ☐ Não ☐ a definir ☐	
Número de Identificação Fiscal	Sim ☐ Não ☐ a definir ☐	
Morada	Sim ☐ Não ☐ a definir ☐	
Filiação Política	Sim ☐ Não ☐ a definir ☐	
Religião	Sim ☐ Não ☐ a definir ☐	
Doenças	Sim ☐ Não ☐ a definir ☐	
Idade	Sim ☐ Não ☐ a definir ☐	
Gênero	Sim ☐ Não ☐ a definir ☐	
Email	Sim ☐ Não ☐ a definir ☐	
Data Nascimento	Sim ☐ Não ☐ a definir ☐	
...	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	

	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	
	Sim ☐ Não ☐ a definir ☐	

PERFIS/NÍVEIS CONTROLO DE ACESSOS

Existem diferentes níveis/perfis de acesso a aplicação/dados: Sim ☐ Não ☐

Se SIM indique os perfis/níveis aplicacionais

Perfil	Nível acesso	Observações
Admin	Ilimitado ☐ Limitado ☐ a definir ☐	
...

DIREITOS DOS UTILIZADORES

Esta contemplado a salvaguarda do registo data/hora dos direitos dos utilizadores? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro______________

Direito	**Estado**	**Formato**	**Observações**
Acesso	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Portabilidade	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Esquecimento	já existe suporte ☐ a criar suporte ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Atualização	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	já existe suporte ☐ a criar ☐ desnecessário ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	

BACKUPS DOS DADOS PESSOAIS – DATA AT REST

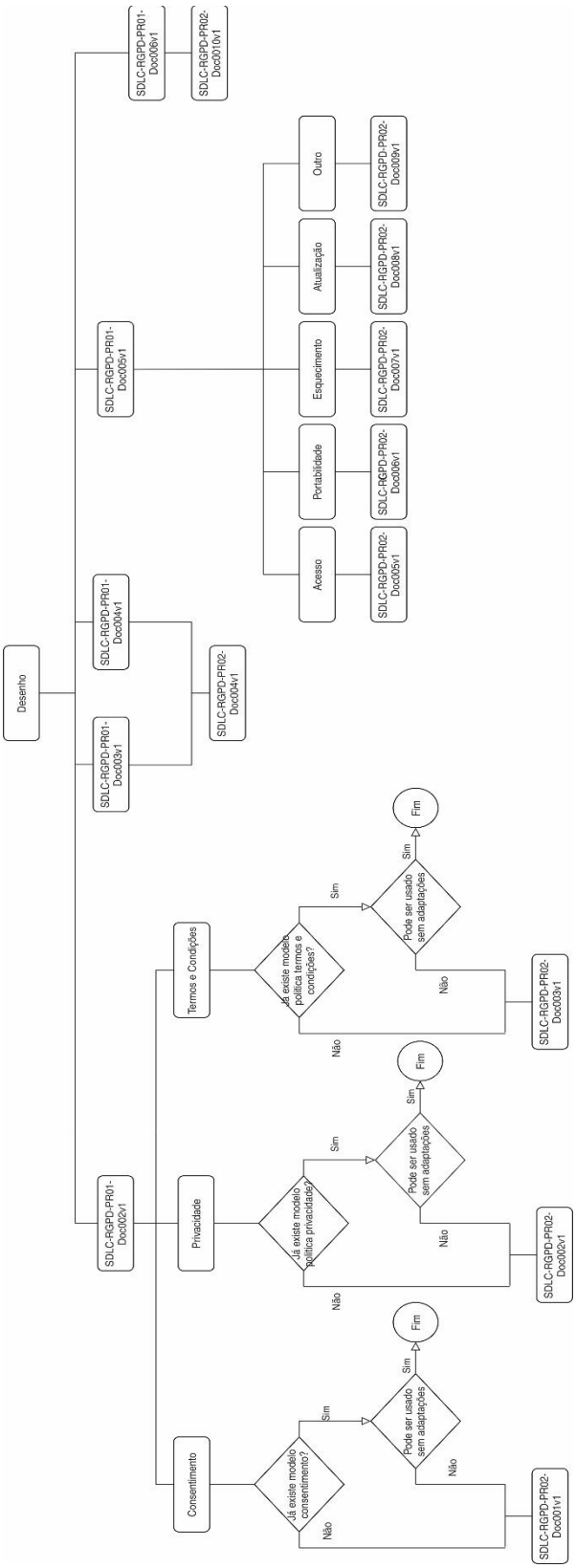
Existem políticas de backup na organização: Sim ☐ Não ☐ N.A. ☐

Devem ser feitos backups dos dados a criar no âmbito da aplicação: Sim ☐ Não ☐

Se SIM descreva o plano de backups:

Tipo	Periodicidade	Tipo	Segurança	Local
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Outro		Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐

Procedimento 2 - Desenho



Documentos de Especificação Desenho:

DESENHO **SDLC-RGPD-PR02-Doc001v1**
FASE SDLC - DESENHO

1. OBJETIVO E ÂMBITO

Incluir no desenho do software aspetos relacionados com o RGPD nomeadamente o consentimento, do titular dos dados pessoais referente ao uso das suas PII.

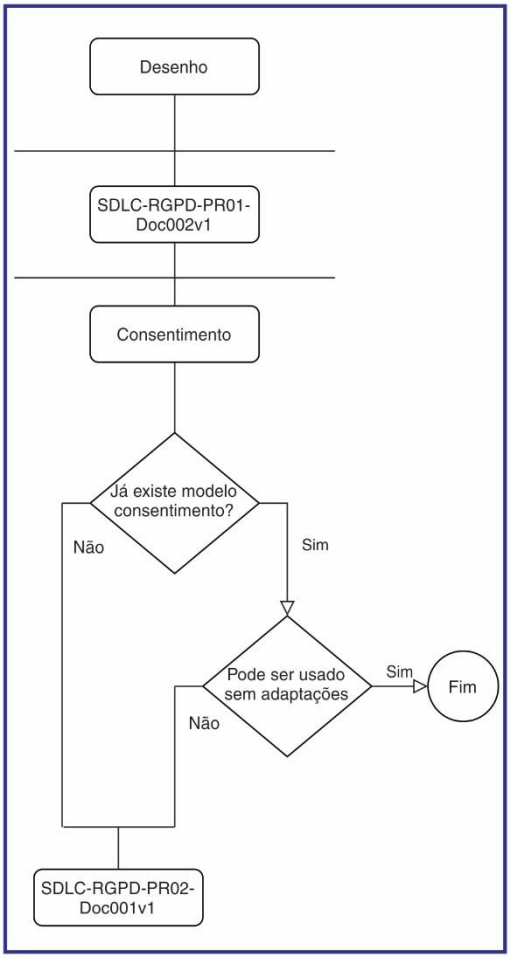
2. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

3. MODO DE PROCEDER

3.1 Documento de Desenho: Doc001v1

3.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Na fase do desenho do SDLC, incluir o RGPD de acordo com as informações recolhidas na análise de requisitos da primeira fase do desenvolvimento do software do documento SDLC-RGPD-PR01-Doc001v1. CONSENTIMENTO Verificar se já existe modelo de consentimento. • Se não existir o modelo de consentimento, preencher o documento de CONSENTIMENTO. • Se existir o modelo de consentimento: Verificar se pode ser usado sem adaptações. • Se sim, é o fim. • Se não, preencher o documento de consentimento.	Desenhista Desenhista Desenhista Desenhista Desenhista Desenhista	SDLC-RGPD-PR02-Doc.001V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

4. OBJETIVO E ÂMBITO

Incluir no desenho do software aspetos relacionados com o RGPD nomeadamente a privacidade dos dados pessoais do titular dos dados pessoais

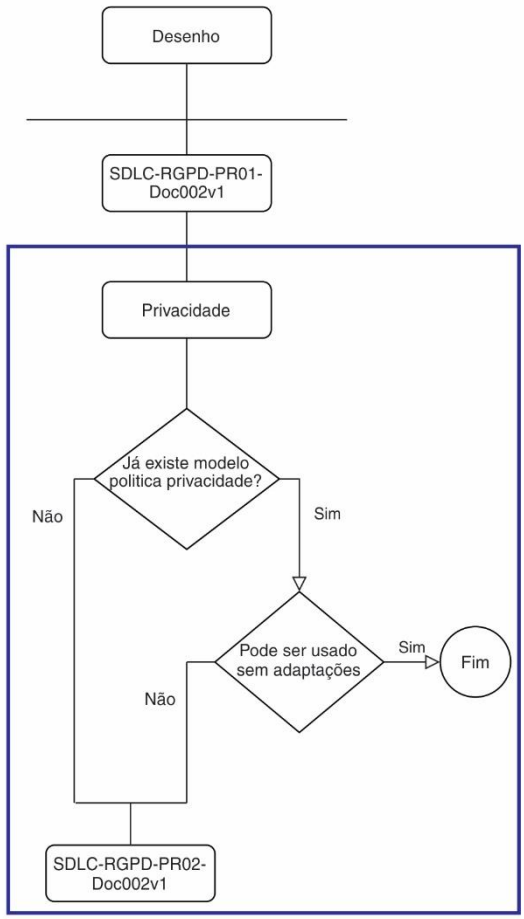
5. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

6. MODO DE PROCEDER

6.1 Documento de Desenho: Doc002v1

6.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	PRIVACIDADE Verificar se já existe modelo de política de privacidade. • Se não existir o modelo de política de privacidade, preencher o documento de PRIVACIDADE. • Se existir o modelo de política de privacidade, verificar se pode ser usado sem adaptações. • Se sim, então é o fim. • Se não, preencher o documento de privacidade.	Desenhista Desenhista Desenhista Desenhista Desenhista	SDLC-RGPD-PR02-Doc.002V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

7. OBJETIVO E ÂMBITO

Incluir no desenho do software aspetos relacionados com o RGPD nomeadamente Termos e Condições para uso dos dados pessoais do titular das PII.

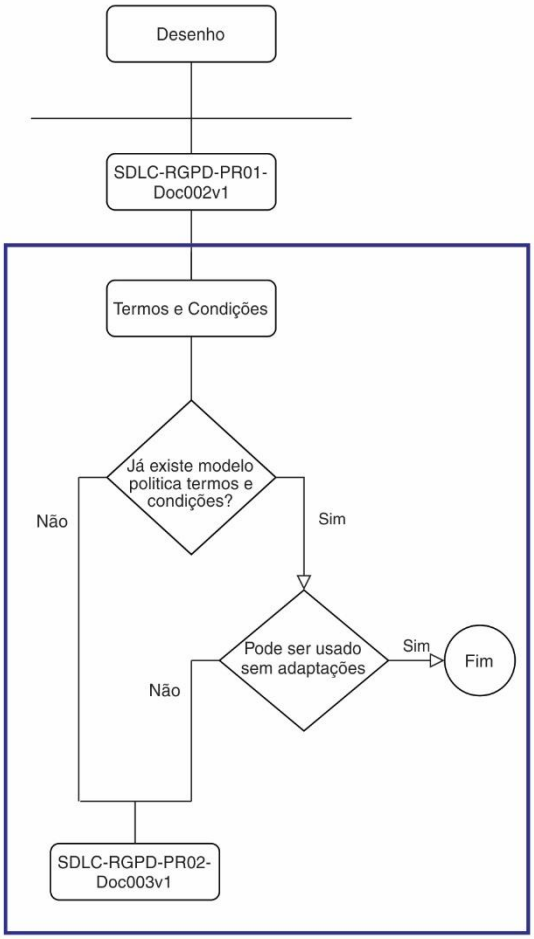
8. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

9. MODO DE PROCEDER

9.1 Documento de Desenho: Doc003v1

9.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	TERMOS E CONDIÇÕES Verificar se já existe modelo de política de termos e condições • Se não existir o modelo de política de termos e condições, deverá preencher o documento TERMOS E CONDIÇÕES. • Se sim, verificar se pode ser usado sem adaptações. • Se sim, então é o fim. • Se não, preencher o documento TERMOS E CONDIÇÕES	Desenhista Desenhista Desenhista Desenhista Desenhista	SDLC-RGPD-PR02-Doc.003V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

10. OBJETIVO E ÂMBITO

Especificar os perfis aplicacionais existentes, que dados são necessários recolher por parte dos utilizadores, onde vão ser armazenados os dados, (matriz).

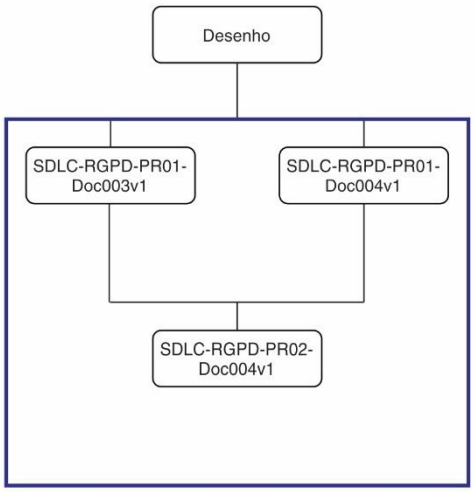
11. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

12. MODO DE PROCEDER

12.1 Documento de Desenho: Doc004v1

12.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se o documento RECOLHA E TRATAMENTO DE DADOS – ESPECIFICAÇÃO DE DADOS (SDLC-RGPD-PR01-Doc003v1) e o documento PERFIS/NÍVEIS CONTROLO DE ACESSOS (SDLC-RGPD-PR01-Doc004v1) estão definidos. • Se ambos os documentos estiverem definidos, então preencher a matriz do documento MATRIZ DE ACESSOS / DADOS (DATA MAPPING).	Desenhista Desenhista	SDLC-RGPD-PR02-Doc.004V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

13. OBJETIVO E ÂMBITO

Acrescentar no desenho do software aspetos relacionados com o RGPD de direito de Acesso aos dados pessoais pelo do titular dos dados, após definir os direitos dos utilizadores de acordo com a análise de requisitos.

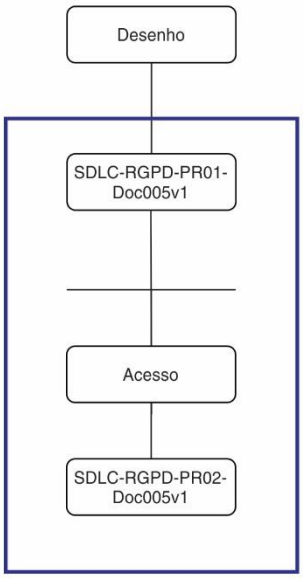
14. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1
BD - Base de Dados

15. MODO DE PROCEDER

15.1 Documento de Desenho: Doc005v1

15.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se o documento DIREITO-TITULARES-DADOS (SDLC-RGPD-PR01-Doc005v1) estão definidos. ACESSO • Preencher o documento de DIREITOS DE ACESSO DOS TITULARES DE PII, definindo o formato, desenho/mockup/ descrição.	Desenhista Desenhista	SDLC-RGPD-PR02-Doc.005V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

16. OBJETIVO E ÂMBITO

Conter no desenho do software aspetos relacionados com o RGPD de direito de Portabilidade dos dados pessoais pelo do titular as PII, após definir os direitos dos utilizadores de acordo com a análise de requisitos.

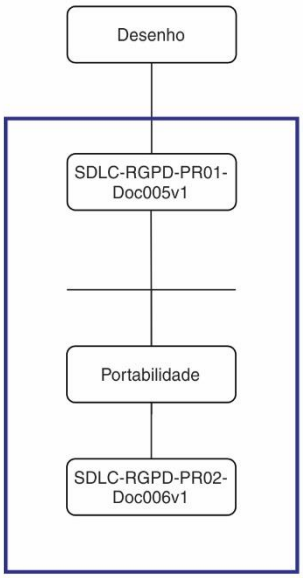
17. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1
BD - Base de Dados

18. MODO DE PROCEDER

18.1 Documento de Desenho: Doc006v1

18.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se o documento DIREITO-TITULARES-DADOS (SDLC-RGPD-PR01-Doc005v1) estão definidos. PORTABILIDADE • Preencher o documento de DIREITOS DE PORTABILIDADE DOS TITULARES DE PII, definindo o formato, desenho/ mockup/descrição.	Desenhista Desenhista	SDLC-RGPD-PR02-Doc.006V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

19. OBJETIVO E ÂMBITO

Conter no desenho do software aspetos relacionados com o RGPD de esquecimento dos dados pessoais do titular dos dados, após definir os direitos dos utilizadores de acordo com a análise de requisitos.

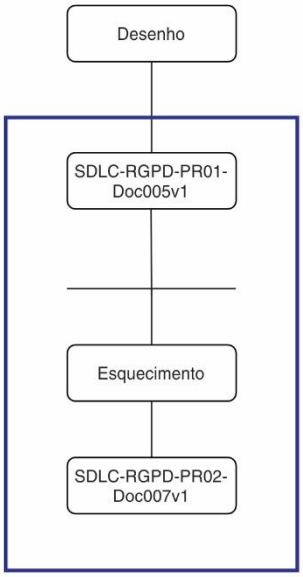
20. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1
BD - Base de Dados

21. MODO DE PROCEDER

21.1 Documento de Desenho: Doc008v1

21.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se o documento DIREITO-TITULARES-DADOS (SDLC-RGPD-PR01-Doc005v1) estão definidos. ESQUECIMENTO • Preencher o documento de DIREITOS DE ESQUECIMENTO das PII, definindo o formato, desenho/ mockup/descrição.	Desenhista Desenhista	SDLC-RGPD-PR02-Doc.007V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

22. OBJETIVO E ÂMBITO

Acrescentar no desenho do software aspetos relacionados com o RGPD da atualização dos dados pessoais do titular dos dados, após definir os direitos dos utilizadores de acordo com a análise de requisitos.

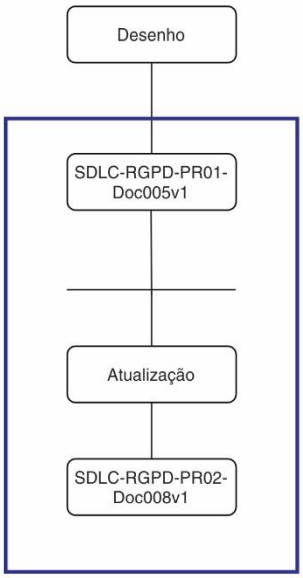
23. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1
BD - Base de Dados

24. MODO DE PROCEDER

24.1 Documento de Desenho: Doc007v1

24.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se o documento DIREITO-TITULARES-DADOS (SDLC-RGPD-PR01-Doc005v1) estão definidos. ATUALIZAÇÃO • Preencher o documento de ATUALIZAÇÃO das PII, definindo o formato, desenho/ mockup/descrição.	Desenhista Desenhista	SDLC-RGPD-PR02-Doc.008V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

25. OBJETIVO E ÂMBITO

Acrescentar no desenho do software aspetos relacionados com o RGPD, referente ao outro tipo de direito solicitado pelo titular dos dados, após definir os direitos dos utilizadores de acordo com a análise de requisitos.

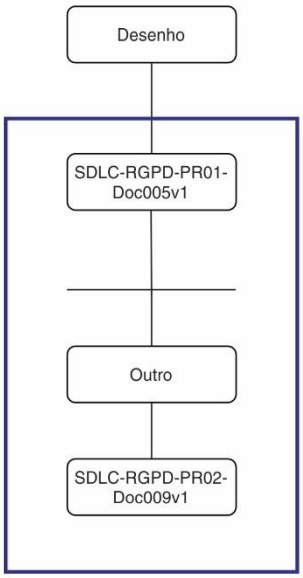
26. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1
BD - Base de Dados

27. MODO DE PROCEDER

27.1 Documento de Desenho: Doc009v1

27.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se o documento DIREITO-TITULARES-DADOS (SDLC-RGPD-PR01-Doc005v1) estão definidos. OUTRO • Preencher o documento de DIREITOS DOS TITULARES DE PII especificar o outro direito requerido pelo titular dos dados, definindo o formato, desenho/ mockup/descrição.	Desenhista Desenhista	SDLC-RGPD-PR02-Doc.009V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

28. OBJETIVO E ÂMBITO

Especificar os perfis aplicacionais existentes, que dados são necessários recolher por parte dos utilizadores, onde vão ser armazenados os dados, (matriz).

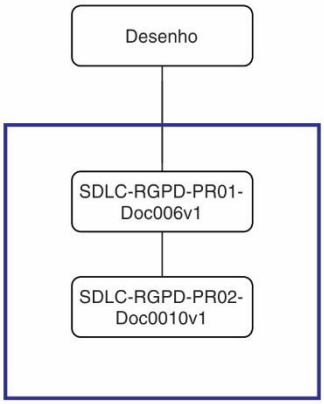
29. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
CC - Cartão Cidadão
Doc - Documento
v1 - Versão 1

30. MODO DE PROCEDER

30.1 Documento de Desenho: Doc0010v1

30.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se os documentos BACKUPS DOS DADOS PESSOAIS – DATA AT REST (SDLC-RGPD-PR01-Doc006v1) está definido. Validar as Informações do BACKUPS DOS DADOS PESSOAIS – DATA AT REST e indicação para fases seguintes.	Desenhista Desenhista	SDLC-RGPD-PR02-Doc.0010V1.

Elaborado por: <Nome do Analista de Sistema>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

CONSENTIMENTO

Está contemplado a salvaguarda do registo data/hora do consentimento? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Existe modelo consentimento explícito? Sim ☐ Não ☐

Pode ser usado sem adaptações? Sim ☐ Não ☐

Texto/desenho do formulário/página a criar

[Desenho/Mockup]

PRIVACIDADE

Esta contemplado a salvaguarda do registo data/hora da privacidade? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Existe modelo política privacidade?	Sim ☐	Não ☐
Pode ser usado sem adaptações?	Sim ☐	Não ☐

Texto/desenho do formulário/página a criar

[Desenho/Mockup]

TERMOS & CONDIÇÕES

Esta contemplado a salvaguarda do registo data/hora do Termos & Condições? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Existe modelo termos e condições?	Sim ☐	Não ☐
Pode ser usado sem adaptações?	Sim ☐	Não ☐

Texto/desenho do formulário/página a criar

[Desenho/Mockup]

MATRIZ DE ACESSOS / DADOS (DATA MAPPING)

INSTRUÇÕES:
Especificar os campos da BD relativos aos dados pessoais/sensíveis na linha 6
Especificar os utilizadores/perfis na coluna A

Completar com S/N sendo "S" indicação de acesso permitido aos campos pelo utilizador/perfis e "N" a indicação de acesso proibido/desnecessário do utilizador/perfil correspondente

User/função / Campo	Primeiro Nome	Sobrenome	Último Nome	Telefone	Morada	Email	NIF	NISS	Género	Empresa	Turno	Data Saída	Localidade	Escolaridade	Estado Civil	Login	Tipo Acesso	Password	Nível	Qualificações	...	...
admin	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	N	S	S		
rh	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	N	S	S		
inf	S	N	S	N	N	N	N	N	S	N	N	N	N	N	N	N	N	N	N	N		
ana@xpto.com	N	N	N	N	N	N	N	N	S	N	N	N	N	N	N	N	N	N	N	N		
manuel@xpto.com	S	N	N	S	N	S	N	N	S	S	S	N	N	N	N	N	N	N	N	N		
DPO	S	S	S	S	N	S	S	S	S	S	S	N	S	S	S	S	S	N	S	S		
...	S	S	S	S	S	S	N	N	S	S	S	N	N	N	N	N	N	N	N	N		
...																						

DIREITOS DOS TITULARES DE PII – **ACESSO**

Está contemplado a salvaguarda do registo data/hora do acesso? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Estado
já existe suporte ☐ a criar ☐ desnecessário ☐

Formato		**Desenho/Mockup/Descrição**
Email	☐	<Indicar o endereço de email através do qual os utilizadores podem efetuar um pedido de acesso à sua PII. Indicar se é para incluir a existência desse endereço de email algum local da aplicação (Menu | termos e condições | privacidade | ...). O email poderá ainda ser desenhado/especificado para o efeito.>
Portal	☐	<Indicar caso já exista o portal/site da empresa através do qual os utilizadores podem efetuar um pedido de acesso à sua PII. Indicar se é para incluir a existência desse portal/site em algum local da aplicação (Menu | termos e condições | privacidade | ...)>
Formulário aplicacional	☐	<Desenhar/especificar o formulário aplicacional a incluir na aplicação que permita, através do mesmo, aos titulares dos dados efetuar um pedido de acesso à sua PII>
Aviso	☐	<Especificar o aviso (página) a apresentar aos utilizadores que pretendam efetuar um pedido de acesso à sua PII ou então a forma como o programador deverá enquadrar tal pedido na aplicação>
Incluído nos avisos legais	☐	<Este caso aplica-se quando a forma de efetuar um pedido de acesso à PII está incluída nos avisos legais podendo ainda ser descrita a forma como o programador deverá enquadrar tal na aplicação>

Outro _____ _____ _____	☐	

DIREITOS DOS TITULARES DE PII – **PORTABILIDADE**

Está contemplado a salvaguarda do registo data/hora da portabilidade? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Estado
já existe suporte ☐ a criar ☐ desnecessário ☐

Formato		**Desenho/Mockup/Descrição**
Email	☐	<Indicar o endereço de email através do qual os utilizadores podem efetuar um pedido de portabilidade de dados. Indicar se é para incluir a existência desse endereço de email em algum local da aplicação (Menu | termos e condições | privacidade | ...). O email poderá ainda ser desenhado/especificado para o efeito.>
Portal	☐	<Indicar, caso já exista, o portal/site da empresa através do qual os utilizadores podem efetuar um pedido de portabilidade de dados. Indicar se é para incluir a existência desse portal/site em algum local da aplicação (Menu | termos e condições | privacidade | ...)>
Formulário aplicacional	☐	<Desenhar/especificar o formulário aplicacional a incluir na aplicação que permita, através do mesmo, aos titulares dos dados efetuar um pedido de portabilidade de PII>
Aviso	☐	<Especificar o aviso (página) a apresentar os utilizadores que pretendam efetuar um pedido de portabilidade de PII ou então a forma como o programador deverá enquadrar tal pedido na aplicação>
Incluído nos avisos legais	☐	<Este caso aplica-se quando a forma de efetuar um pedido de portabilidade de dados está incluída nos avisos legais podendo ainda ser descrita a forma como o programador deverá enquadrar tal na aplicação>
Outro _____ _____	☐	

_____		

DIREITOS DOS TITULARES DE PII – **ESQUECIMENTO**

Está contemplado a salvaguarda do registo data/hora do pedido de esquecimento? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Estado
já existe suporte ☐ a criar ☐ desnecessário ☐

Formato		**Desenho/Mockup/Descrição**
Email	☐	<Indicar o endereço de email através do qual os utilizadores podem efetuar um pedido de esquecimento à sua PII. Indicar se é para incluir a existência desse endereço de email em algum local da aplicação (Menu | termos e condições | privacidade | ...). O email poderá ainda ser desenhado/especificado para o efeito.>
Portal	☐	<Indicar caso já exista o portal/site da empresa através do qual os utilizadores podem efetuar um pedido de esquecimento da sua PII. Indicar se é para incluir a existência desse portal/site em algum local da aplicação (Menu | termos e condições | privacidade | ...)>
Formulário aplicacional	☐	<Desenhar/especificar o formulário aplicacional a incluir na aplicação que permita, através do mesmo, aos titulares dos dados efetuar um pedido de esquecimento das suas PII>
Aviso	☐	<Especificar o aviso (página) a apresentar aos utilizadores que pretendam efetuar um pedido de esquecimento das suas PII ou então a forma como o programador deverá enquadrar tal pedido na aplicação>
Incluído nos avisos legais	☐	<Este caso aplica-se quando a forma de efetuar um pedido de esquecimento das PII está incluída nos avisos legais podendo ainda ser descrita a forma como o programador deverá enquadrar tal na aplicação>
Outro _____ _____	☐	

_____		

DIREITOS DOS TITULARES DE PII – **ATUALIZAÇÃO**

Está contemplado a salvaguarda do registo data/hora da atualização? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Estado
já existe suporte ☐ a criar ☐ desnecessário ☐

Formato		**Desenho/Mockup/Descrição**
Email	☐	<Indicar o endereço de email através do qual os utilizadores podem efetuar um pedido de atualização das suas PII. Indicar se é para incluir a existência desse endereço de email algum local da aplicação (Menu | termos e condições | privacidade | ...). O email poderá ainda ser desenhado/especificado para o efeito.>
Portal	☐	<Indicar caso já exista o portal/site da empresa através do qual os utilizadores podem efetuar um pedido de atualização das suas PII. Indicar se é para incluir a existência desse portal/site em algum local da aplicação (Menu | termos e condições | privacidade | ...)>
Formulário aplicacional	☐	<Desenhar/especificar o formulário aplicacional a incluir na aplicação que permita, através do mesmo, aos titulares dos dados efetuar um pedido de atualização dos seus dados>
Aviso	☐	<Especificar o aviso (página) a apresentar os utilizadores que pretendam efetuar um pedido de atualização das suas PII ou então a forma como o programador deverá enquadrar tal pedido na aplicação>
Incluído nos avisos legais	☐	<Este caso aplica-se quando a forma de efetuar um pedido de atualização das PII está incluída nos avisos legais podendo ainda ser descrita a forma como o programador deverá enquadrar tal na aplicação>
Outro _____ _____	☐	

_____		

DIREITOS DOS TITULARES DE PII – **<ESPECIFICAR>**

Está contemplado a salvaguarda do registo data/hora do <ESPECIFICAR>? ☐ Sim ☐ Não

Qual a forma? ☐ Base de dados ☐ Email ☐ Aplicação especifica RGPD ☐ Outro_____

Estado
já existe suporte ☐ a criar ☐ desnecessário ☐

Formato		**Desenho/Mockup/Descrição**
Email	☐	
Portal	☐	
Formulário aplicacional	☐	
Aviso	☐	
Incluído nos avisos legais	☐	
Outro _____ _____ _____	☐	

BACKUPS DOS DADOS PESSOAIS – DATA AT REST

1 - Informação recolhida da fase de análise e especificação de requisitos

Existem políticas de backup na organização: Sim ☐ Não ☐ N.A. ☐

Devem ser feitos backups dos dados a criar no âmbito da aplicação: Sim ☐ Não ☐

Se SIM descreva o plano de backups:

Tipo	Periodicidade	Tipo	Segurança	Local
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Outro		Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐

2 – Validação da Informação e indicação para fases seguintes

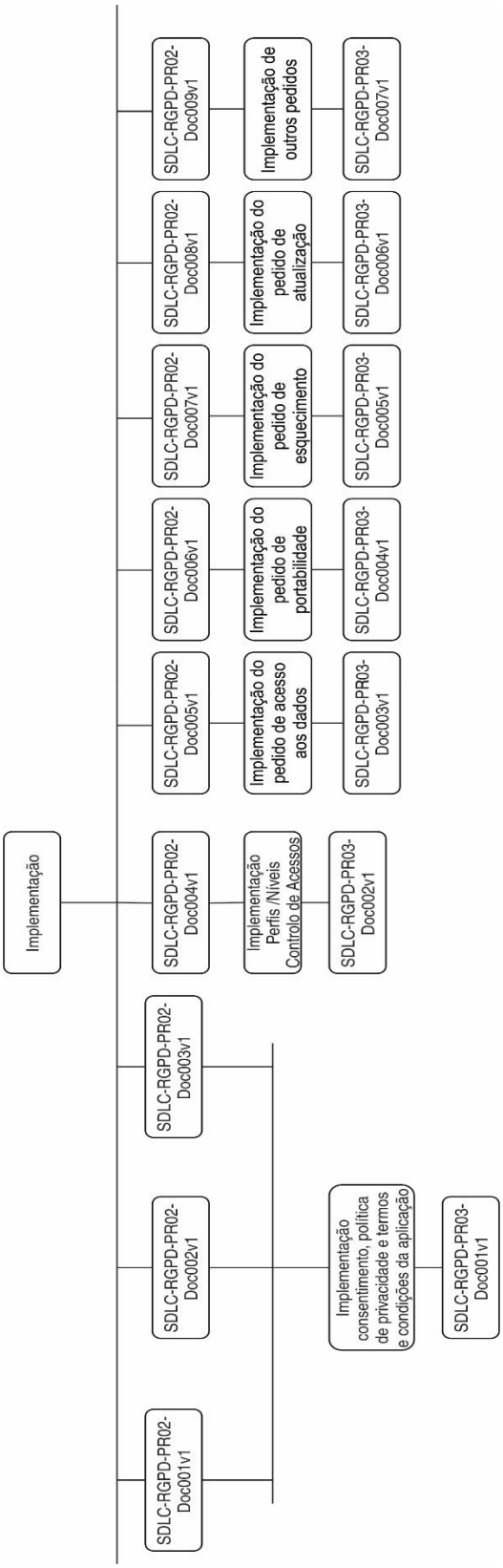
Valido a informação relativa aos backups: Sim ☐ Não ☐

Plano(s) de backups a implementar:

Tipo	Periodicidade	Tipo	Segurança	Local	Impl
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro ____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro ____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
...		Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐

Observações:

Procedimento 3 - Implementação



Documentos de Especificação Implementação:

1. OBJETIVO E ÂMBITO

Codificação do software de acordo com os princípios do RGPD (identificados na fase de desenho).
Implementar na aplicação os modelos de consentimento, privacidade, termos e condições da aplicação.

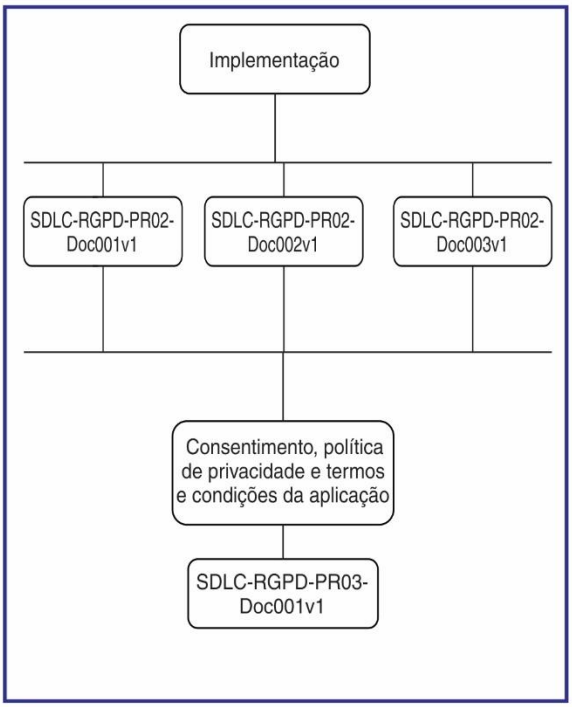
2. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

3. MODO DE PROCEDER

3.1 Documento de Implementação: Doc001v1

3.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Na fase da Implementação do SDLC, incluir o RGPD na codificação do software de acordo com as informações recolhidas na fase de desenho, com os documentos definidos na fase anterior. De acordo com o documento de consentimento, política de privacidade e termos e condições da aplicação. Implementar os modelos na aplicação de consentimento, privacidade, termos e condições da aplicação e indicar no documento Consentimento, Privacidade, Termos & Condições.	Desenvolvedor Desenvolvedor Desenvolvedor	SDLC-RGPD-PR03-Doc.001V1.

Elaborado por: <Nome do Desenvolvedor>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

4. OBJETIVO E ÂMBITO

Seguir o documento matriz da fase do desenho e implementar o controlo de acessos considerando os perfis e o acesso a dados. Considerar o local de armazenamento de dados com cifra forte.

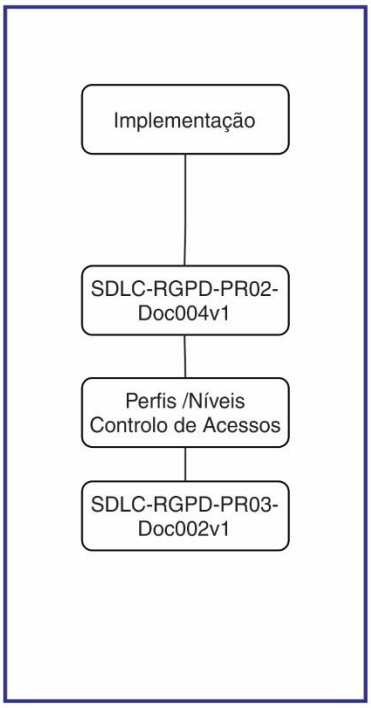
5. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

6. MODO DE PROCEDER

6.1 Documento de Implementação: Doc002v1

6.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	De acordo com o documento Matriz de Acessos / Dados (Data Mapping), implementar o Controlo de Acesso aos Dados Pessoais. Especificar no documento Controlo de Acesso aos Dados Pessoais os Perfis/Níveis Controlo de Acesso que foram implementados de acordo com a Matriz de Acesso do desenho e informar se a base de dados está ou não protegida com mecanismos de cifra e qual controlo adotado para o utilizador / perfil e campo da BD.	Desenvolvedor Desenvolvedor	SDLC-RGPD-PR03-Doc.002V1.

Elaborado por: <Nome do Desenvolvedor>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

7. OBJETIVO E ÂMBITO

Implementação do direito de acesso aos dados pessoais por parte dos utilizadores, seguindo o documento da fase desenho SDLC-RGPD-PR02-Doc005v1

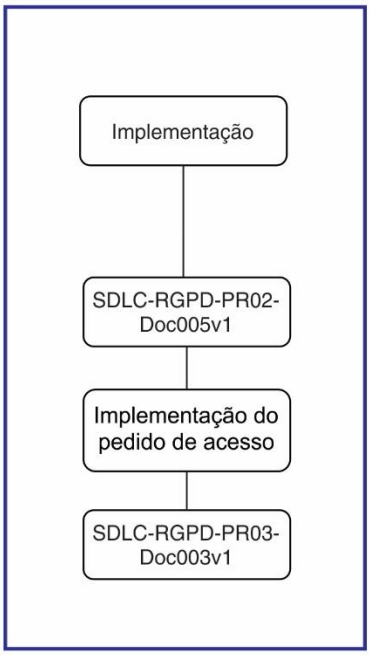
8. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

9. MODO DE PROCEDER

9.1 Documento de Implementação: Doc003v1

9.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Seguir o documento da fase desenho DIREITOS DOS TITULARES DE PII - ACESSO. Preencher documento Implementação do pedido de acesso aos dados pessoais. Se foi implementado, indicar a forma que foi usada. Se não foi implementado, indicar o motivo.	Desenvolvedor Desenvolvedor Desenvolvedor Desenvolvedor	SDLC-RGPD-PR03-Doc.003V1.

Elaborado por: <Nome do Desenvolvedor>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

10. OBJETIVO E ÂMBITO

Implementação do direito de portabilidade dos dados pessoais por parte dos utilizadores, seguindo o documento da fase desenho SDLC-RGPD-PR02-Doc006v1

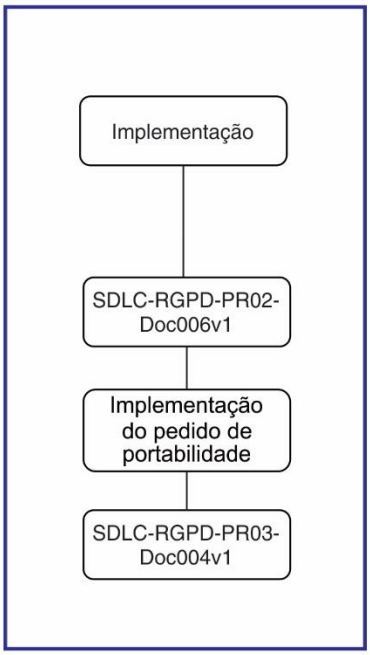
11. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

12. MODO DE PROCEDER

12.1 Documento de Implementação: Doc004v1

12.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Seguir o documento da fase desenho DIREITOS DOS TITULARES DE PII - PORTABILIDADE. Preencher documento Implementação do pedido de portabilidade dos dados pessoais. Se foi implementado, indicar a forma que foi usada. Se não foi implementado, indicar o motivo.	Desenvolvedor Desenvolvedor Desenvolvedor Desenvolvedor	SDLC-RGPD-PR03-Doc.004V1.

Elaborado por: <Nome do Desenvolvedor>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

13. OBJETIVO E ÂMBITO

Implementação do direito de esquecimento dos dados pessoais por parte dos utilizadores, seguindo o documento da fase desenho SDLC-RGPD-PR02-Doc007v1

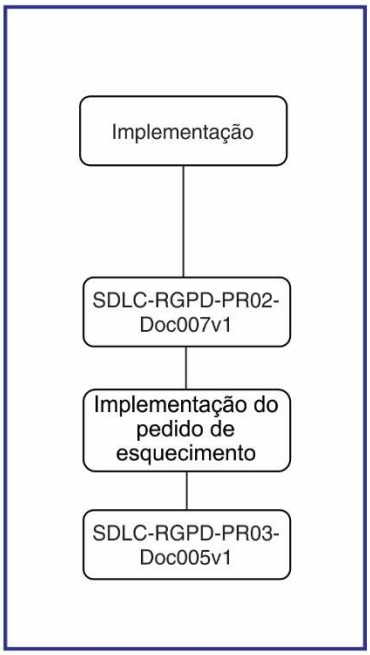
14. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

15. MODO DE PROCEDER

15.1 Documento de Implementação: Doc005v1

15.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Seguir o documento da fase desenho DIREITOS DOS TITULARES DE PII - ESQUECIMENTO. Preencher documento Implementação do pedido de esquecimento dos dados pessoais. Se foi implementado, indicar a forma que foi usada. Se não foi implementado, indicar o motivo.	Desenvolvedor Desenvolvedor Desenvolvedor Desenvolvedor	SDLC-RGPD-PR03-Doc.005V1.

Elaborado por: <Nome do Desenvolvedor>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

16. OBJETIVO E ÂMBITO

Implementação do direito de atualização dos dados pessoais por parte dos utilizadores, seguindo o documento da fase desenho SDLC-RGPD-PR02-Doc008v1

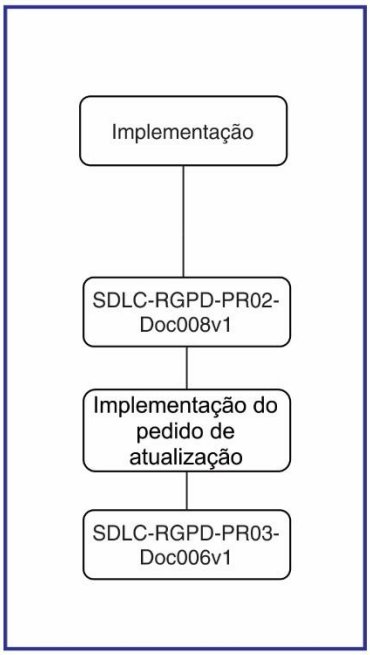
17. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

18. MODO DE PROCEDER

18.1 Documento de Implementação: Doc006v1

18.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Seguir o documento da fase desenho DIREITOS DOS TITULARES DE PII - ATUALIZAÇÃO. Preencher documento Implementação do pedido de atualização dos dados pessoais. Se foi implementado, indicar a forma que foi usada. Se não foi implementado, indicar o motivo.	Desenvolvedor Desenvolvedor Desenvolvedor Desenvolvedor	SDLC-RGPD-PR03-Doc.006V1.

Elaborado por: <Nome do Desenvolvedor>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

19. OBJETIVO E ÂMBITO

Implementação de outros pedidos referente aos dados pessoais por parte dos utilizadores, seguindo o documento da fase desenho SDLC-RGPD-PR02-Doc009v1

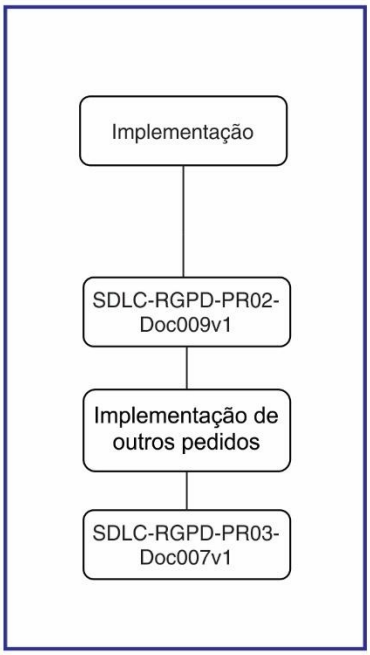
20. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

21. MODO DE PROCEDER

21.1 Documento de Implementação: Doc007v1

21.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Seguir o documento da fase desenho DIREITOS DOS TITULARES DE PII - <ESPECIFICAR>. Preencher documento Implementação de outros pedidos referente aos dados pessoais. Se foi implementado, indicar a forma que foi usada. Se não foi implementado, indicar o motivo.	Desenvolvedor Desenvolvedor Desenvolvedor Desenvolvedor	SDLC-RGPD-PR03-Doc.007V1.

Elaborado por: <Nome do Desenvolvedor>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

CONSENTIMENTO, PRIVACIDADE E TERMOS & CONDIÇÕES

Foi implementado o consentimento de recolha e tratamento PII? Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link	☐	Observações: indique aqui o link, *template* de email ou forma usada na implementação do consentimento de recolha e tratamento de dados pessoais. Caso tenha feito alterações ao modelo de consentimento recebido em fases anteriores indique aqui que alterações fez.
	Formulário	☐	
	Email	☐	
	Outro	☐	

Como está a ser guardado o consentimento?	
Não está a ser guardado	☐
Está a ser guardado	☐ (indicar abaixo como)
Observações:	

Se foi pedido e NÃO foi implementado, diga o porquê:

Foi implementado na aplicação o modelo política privacidade? Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link	☐	Observações: indique aqui o link, *template* de email ou forma usada na implementação/divulgação da política de privacidade em vigor na empresa. Caso tenha feito alterações ao modelo recebido em fases anteriores indique aqui que alterações foram feitas.
	Formulário	☐	
	Email	☐	
	Outro	☐	

Como está a ser guardado o acordo (check) com a política de privacidade?	
Não está a ser guardado	☐
Está a ser guardado	☐ (indicar abaixo como)
Observações:	

Se foi pedido e NÃO foi implementado, diga o porquê:

Foi implementado na aplicação o modelo termos e condições? Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link	☐	Observações: indique aqui o link, *template* de email ou forma usada na implementação/divulgação do termos e condições da utilização da aplicação. Caso tenha feito alterações ao modelo recebido em fases anteriores indique aqui que alterações fez.
	Formulário	☐	
	Email	☐	
	Outro	☐	

Como está a ser guardado o acordo (check) com os termos e condições apresentados?	
Não está a ser guardado	☐
Está a ser guardado	☐ (indicar abaixo como)
Observações:	

Se foi pedido e NÃO foi implementado, diga o porquê:

CONTROLO DE ACESSO AOS DADOS PESSOAIS
DE ACORDO COM MATRIZ DE ACESSOS / DADOS (DATA MAPPING)

O controle de acesso foi implementado de acordo com a Matriz de Acessos / Dados? Sim ☐ Não ☐ Parcialmente ☐ Não se aplica ☐

A BD está protegida através de mecanismos de cifra? Sim ☐ Não ☐

Se implementou integralmente ou parcialmente o controlo de acessos indique:

Utilizador/Perfil e Campo(s) da BD	**Query/Vista implementada**	**Controlo adotado** **(ofuscação, anonimização, ...)**
		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____

		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____
		Ofuscação☐ Anonimização☐ Outro☐ _____

IMPLEMENTAÇÃO DO PEDIDO
DE ACESSO AOS DADOS

Foi implementado o **direito de acesso** aos dados do utilizador?

Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link		Observações: indique a forma usada na implementação do direito de acesso aos dados pessoais por parte dos utilizadores. Caso tenha feito alterações ao documento SDLC-RGPD-PR02-Doc005v1 indique aqui que alterações fez.
	Formulário		
	Email		
	Outro		

Se foi pedido e NÃO foi implementado, diga o porquê:

IMPLEMENTAÇÃO DO PEDIDO
DE PORTABILIDADE

Foi implementado o **direito de portabilidade** aos dados do utilizador?

Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link		Observações: indique a forma usada na implementação do direito de portabilidade aos dados pessoais por parte dos utilizadores. Caso tenha feito alterações ao documento SDLC-RGPD-PR02-Doc006v1 indique aqui que alterações fez.
	Formulário		
	Email		
	Outro		

Se foi pedido e NÃO foi implementado, diga o porquê:

IMPLEMENTAÇÃO DO PEDIDO
DE ESQUECIMENTO

Foi implementado o **direito de esquecimento** aos dados do utilizador?

Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link		Observações: indique a forma usada na implementação do direito de esquecimento aos dados pessoais por parte dos utilizadores. Caso tenha feito alterações ao documento SDLC-RGPD-PR02-Doc007v1 indique aqui que alterações fez.
	Formulário		
	Email		
	Outro		

Se foi pedido e NÃO foi implementado, diga o porquê:

IMPLEMENTAÇÃO DO PEDIDO
DE ATUALIZAÇÃO

Foi implementado o **direito de atualização** aos dados do utilizador?

Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link		Observações: indique a forma usada na implementação do direito de atualização aos dados pessoais por parte dos utilizadores. Caso tenha feito alterações ao documento SDLC-RGPD-PR02-Doc008v1 indique aqui que alterações fez.
	Formulário		
	Email		
	Outro		

Se foi pedido e NÃO foi implementado, diga o porquê:

IMPLEMENTAÇÃO DE
OUTROS PEDIDOS **<ESPECIFICAR>**

Foi implementado **outro direito** aos dados do utilizador?

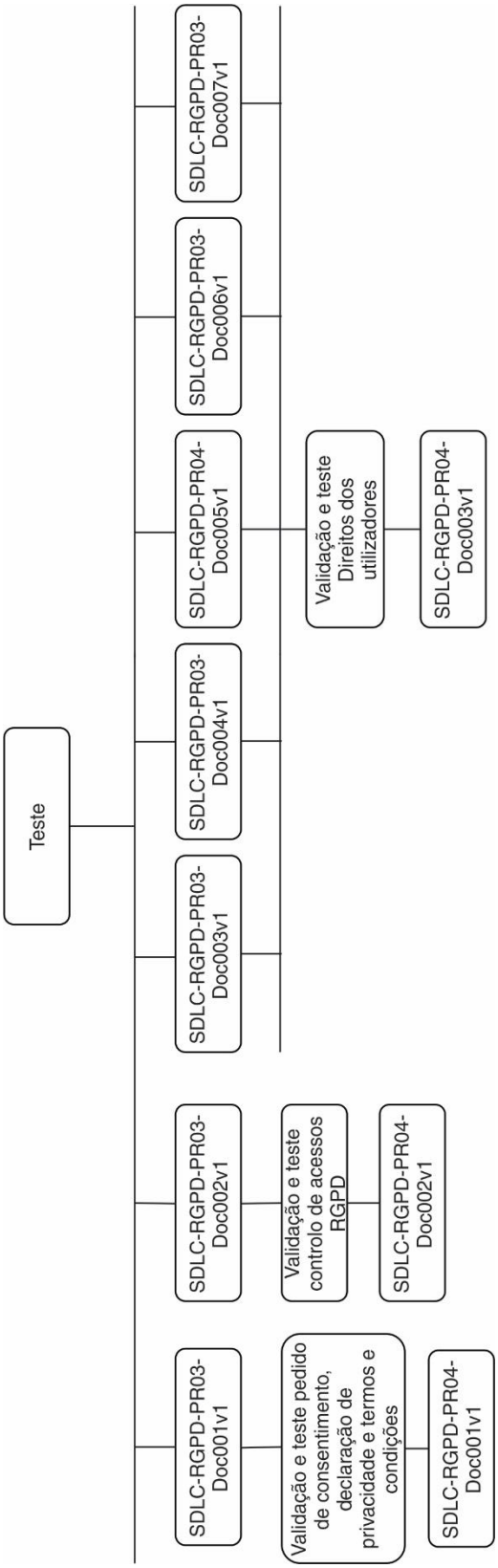
Sim ☐ Não ☐ Não se aplica ☐

Se SIM indique:

De que forma foi implementado?	Página web e link		Observações: indique a forma usada na implementação do outro direito <ESPECIFICAR> aos dados pessoais por parte dos utilizadores. Indicar alterações ao documento SDLC-RGPD-PR02-Doc009v1.
	Formulário		
	Email		
	Outro		

Se foi pedido e NÃO foi implementado, diga o porquê:

Procedimento 4 – Teste



1. OBJETIVO E ÂMBITO

Auditoria à aplicação e base de dados com enfoque na PII. Validação e teste pedido de consentimento, declaração de privacidade e termos e condições

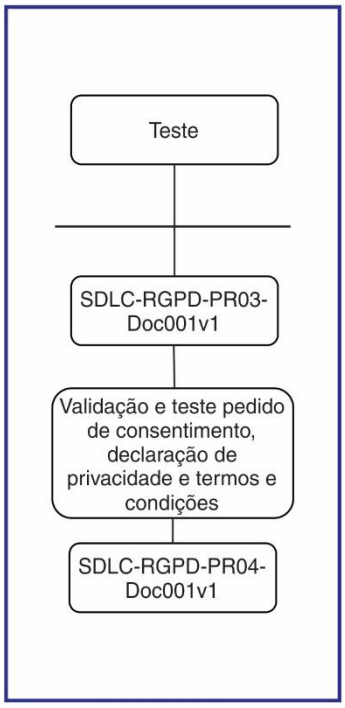
2. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

3. MODO DE PROCEDER

3.1 Documento de Teste: Doc001v1

3.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Na fase do Teste do SDLC, verificar se implementação atende ao RGPD através de uma auditoria de segurança, com enfoque na proteção das informações pessoais do titular dos dados. De acordo com o documento CONSENTIMENTO, PRIVACIDADE E TERMOS & CONDIÇÕES preenchido na fase de implementação: Realizar os testes e preencher o documento de validação e teste pedido de consentimento, declaração de privacidade e termos e condições	Equipa Teste Equipa Teste Equipa Teste	SDLC-RGPD-PR04-Doc.001V1.

Elaborado por:	Verificado por:	Aprovado por:
<Nome do Responsável pelo Teste>	<Nome do DPO>	<Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

4. OBJETIVO E ÂMBITO

Auditoria à aplicação e base de dados com enfoque na PII. Controlo de perfil e acesso, validação e teste de acordo com o RGPD.

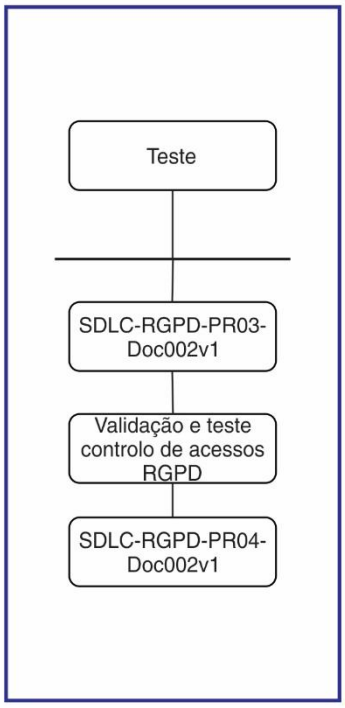
5. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

6. MODO DE PROCEDER

6.1 Documento de Teste: Doc002v1

6.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	De acordo com o documento CONTROLE DE ACESSO AOS DADOS PESSOAIS DE ACORDO COM MATRIZ DE ACESSOS / DADOS (DATA MAPPING) preenchido na fase de implementação: Realizar os testes e preencher o documento validação e teste controlo de acessos RGPD com os resultados.	Equipa Teste Equipa Teste	SDLC-RGPD-PR04-Doc.002V1.

Elaborado por: <Nome do Responsável pelo Teste>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

7. OBJETIVO E ÂMBITO

Auditoria à aplicação e base de dados com enfoque na PII.
Validação e teste dos direitos dos utilizadores sobre os dados pessoais (direito de acesso, direito de portabilidade, direito de esquecimento, direito de atualização ou outro direito implementado)

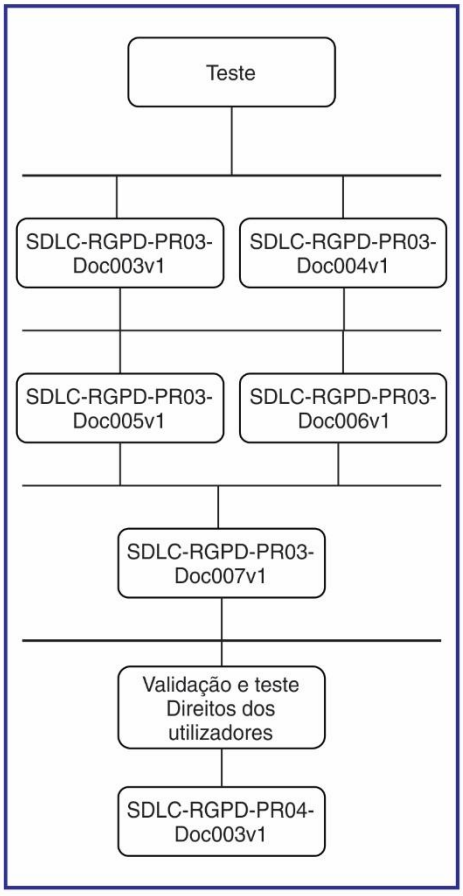
8. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

9. MODO DE PROCEDER

9.1 Documento de Teste: Doc003v1

9.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	De acordo com os documentos IMPLEMENTAÇÃO DO PEDIDO DE ACESSO AOS DADOS, PEDIDO DE PORTABILIDADE, PEDIDO DE ESQUECIMENTO, ATUALIZAÇÃO, OUTROS PEDIDOS, preenchidos na fase de implementação: Realizar os testes e preencher o documento Validação e Teste Direitos dos utilizadores com os resultados.	Equipa Teste Equipa Teste	SDLC-RGPD-PR04-Doc.003V1.

Elaborado por: <Nome do Responsável pelo Teste>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

VALIDAÇÃO E TESTE PEDIDO DE CONSENTIMENTO,
DECLARAÇÃO DE PRIVACIDADE E TERMOS E CONDIÇÕES

Pedido de consentimento ao titular do dados:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações: <indicar motivo de não conformidade>

Declaração de privacidade dos dados:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações: <indicar motivo de não conformidade>

Termos e condições:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações: <indicar motivo de não conformidade>

Resultado do teste:

VALIDAÇÃO E TESTE CONTROLO DE ACESSOS RGPD

Perfil/ Utilizador	**Formulário/Opção**	**Controlo adotado** **(ofuscação, anonimização, ...)**	**Validação/Teste**	**Observações**
		Ofuscação ☐ Anonimização ☐ Outro ☐ ______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ ______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ ______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ ______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	

		Ofuscação ☐ Anonimização ☐ Outro ☐ _______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ _______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ _______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ _______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	
		Ofuscação ☐ Anonimização ☐ Outro ☐ _______________	Implementado ☐ Testado ☐ Conforme ☐ Não Conforme ☐	

VALIDAÇÃO E TESTE DIREITOS
DOS UTILIZADORES

Pedido de **acesso** aos dados pessoais:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações:

Pedido de **portabilidade** dos dados pessoais:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações:

Pedido de **esquecimento** dos dados pessoais por parte do titular dos dados:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações:

Pedido de **atualização** dos dados pessoais por parte do titular dos dados:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

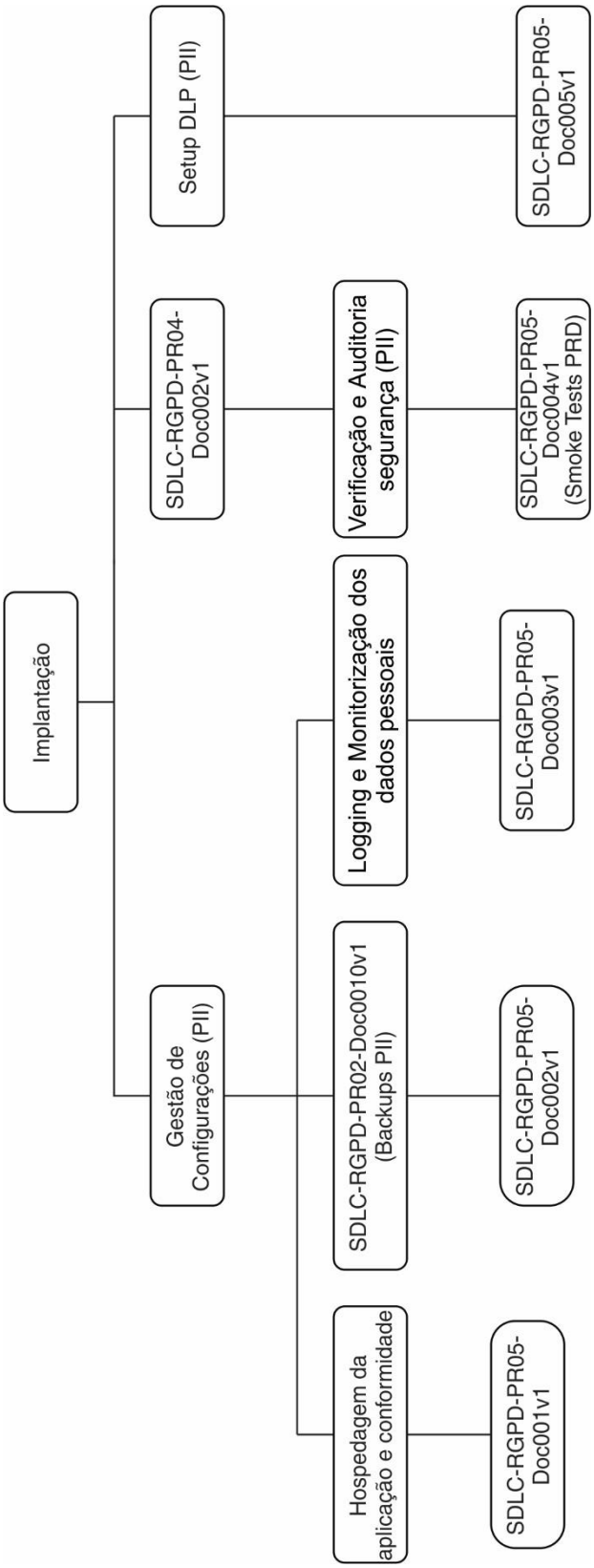
Observações:

Outro tipo de pedido sobre os dados pessoais por parte do titular dos dados:
Implementado ☐ Testado ☐ Conforme ☐ Não conforme ☐

Observações:

Resultado do teste:

Procedimento 5 - Implantação



Documentos de Especificação Implantação:

IMPLANTAÇÃO **SDLC-RGPD-PR05-Doc001v1**
FASE SDLC - IMPLANTAÇÃO

1. OBJETIVO E ÂMBITO

Disponibilizar a aplicação em ambiente de produção com os mecanismos para proteção de riscos e proteção da PII. Realizar a Gestão de Configurações (PII) e verificar a Hospedagem da aplicação e conformidade com o RGPD.

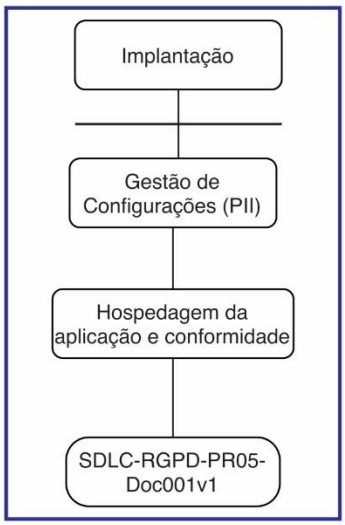
2. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1
DLP - Prevenção de perda de dados

3. MODO DE PROCEDER

3.1 Documento de Implantação Doc001v1

3.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Na fase Implantação do SDLC, após passar pela auditoria do teste em conformidade com o RGPD , realizar a Gestão de Configurações (PII).	Equipa Produção	SDLC-RGPD-PR05-Doc.001V1.
	Preencher o documento HOSPEDAGEM DA APLICAÇÃO E CONFORMIDADE, de acordo com o Alojamento da Aplicação (binários) e verificar o tipo de hospedagem, tipo do alojamento, a Consola de gestão e se estão em conformidade ou não com o RGPD.	Equipa Produção	
	Também preencher a tabela Alojamento dados Aplicação(Storage) e verificar o se o Storage é Interno ou externo, tipo de Storage, Consola de gestão e a presença ou não de conformidade com o RGPD.	Equipa Produção	

Elaborado por: <Nome do Responsável pela Implantação>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

4. OBJETIVO E ÂMBITO

Também na Gestão de Configurações (PII), seguindo o documento de backup da fase de desenho validado, verificar se os Backups PII estão em conformidade com o RGPD garantindo a segurança dos dados pessoais.

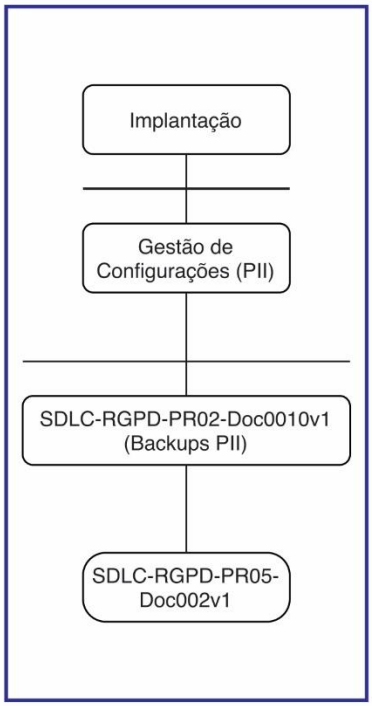
5. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1
DLP - Prevenção de perda de dados

6. MODO DE PROCEDER

6.1 Documento de Implantação Doc002v1

6.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Continuar a Gestão de Configurações (PII) da fase de implantação para verificar conformidade dos backups de acordo com o RGPD. Seguindo o documento validado na fase desenho referente aos Backups das PII, também preencher o documento BACKUPS DADOS PESSOAIS na fase de implantação da aplicação. Verificar se os backups são internos ou externos, Tipo de backup. Além disso, assinalar se os backups e reposição foram testados e se foram implementados de acordo com o plano.	Equipa Produção Equipa Produção Equipa Produção	SDLC-RGPD-PR05-Doc.002V1.

Elaborado por: <Nome do Responsável pela Implantação>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

7. OBJETIVO E ÂMBITO

Dentre os documentos da Gestão de Configurações (PII), encontra-se o documento para fazer a verificação do Logging e monitorização de dados pessoais, garantindo o registro de acesso às PII.

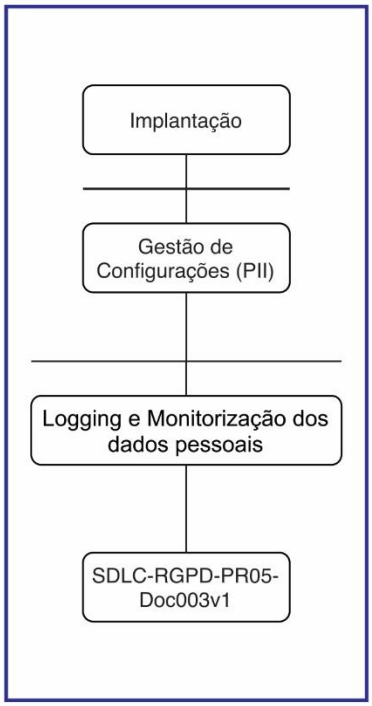
8. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1
DLP - Prevenção de perda de dados

9. MODO DE PROCEDER

9.1 Documento de Implantação Doc003v1

9.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Ainda na Gestão de Configurações (PII) da fase implantação, conferir o Logs e Monitorização dos dados pessoais se estão de acordo com o regulamento.	Equipa Produção	SDLC-RGPD-PR05-Doc.003V1.
	Preencher o documento LOGGING E MONITORIZAÇÃO DE DADOS PESSOAIS.	Equipa Produção	
	Verificar o controle de acesso registrado em log, monitorização de log e de acesso aos dados, acesso(ler, alterar, remover) e os direitos exercido pelos utilizadores armazenados em log.	Equipa Produção	

Elaborado por: <Nome do Responsável pela Implantação>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

10. OBJETIVO E ÂMBITO

Após ser validado o teste controlo de acessos RGPD no documento da fase anterior, realizar a verificação e auditoria de segurança (PII) baseado no Smoke Test PRD, informando os tipos de filtro, log de acesso, log de direto, soluções DLP e backups, de segurança de acordo com o RGPD.

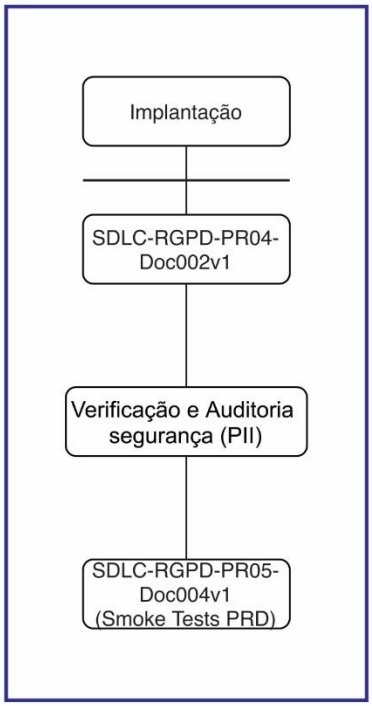
11. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1
DLP - Prevenção de perda de dados

12. MODO DE PROCEDER

12.1 Documento de Implantação Doc004v1

12.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar o documento preenchido na fase teste, Validação e teste controlo de acessos RGPD. Preencher o documento VERIFICAÇÃO E AUDITORIA DE SEGURANÇA (PII) (SMOKE TESTS PRD). Verificar se os dados são filtrados de acordo com o perfil aplicacional. Caso positivo, informar o tipo de filtro aplicado. Informar o tipo de log de acesso a aplicação, log dos direitos, forma como é feita reposição de um backup, segurança dos backups dos dados pessoais e a solução DLP.	Equipa Produção Equipa Produção Equipa Produção	SDLC-RGPD-PR05-Doc.004V1.

Elaborado por: <Nome do Responsável pela Implantação>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

13. OBJETIVO E ÂMBITO

Realizar o preenchimento
do documento de setup DLP (PII)
e verificar se existe algo na aplicação
que afeta o DLP e os tipos de controlos
ativados para a aplicação ficar em
conformidade com o RGPD, validando
a implantação do sistema.

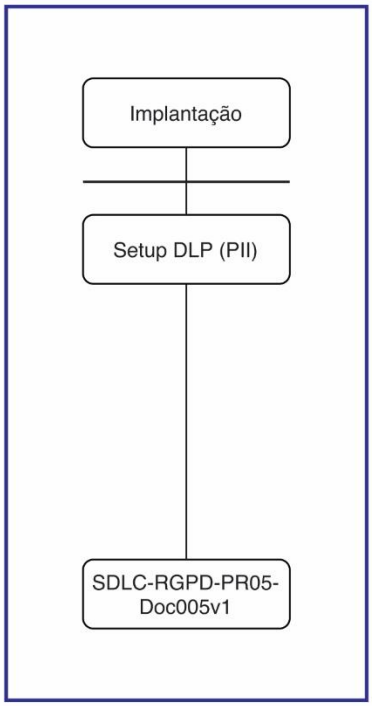
14. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1
DLP - Prevenção de perda de dados

15. MODO DE PROCEDER

15.1 Documento de Implantação Doc005v1

15.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Preencher o documento SOLUÇÃO DATA LOSS PREVENTION, verificar se existe alguma solução na aplicação que afeta DLP. Caso exista, identificar os controlos e se estão ou não ativados no sistema. Também identificar os tipos de monitorização cobertos pela solução de DLP e os exemplos de controlos ativados.	Equipa Produção Equipa Produção	SDLC-RGPD-PR05-Doc.005V1.

Elaborado por: <Nome do Responsável pela Implantação>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

ALOJAMENTO APLICAÇÃO (Binários)

Hospedagem	Tipo alojamento	Consola de Gestão	Conformidade RGPD
Interno ☐	Servidor Dedicado ☐ Servidor Partilhado ☐ Cloud Privada ☐ Outro ☐ _____	Acesso Pessoal Interno ☐ Acesso Pessoal Externo ☐ Outro ☐ _____	Sim ☐ Não ☐ N.A. ☐
Externo ☐	Servidor Dedicado ☐ Servidor Partilhado ☐ Cloud Privada ☐ Cloud Pública ☐ Outro ☐ _____	Acesso Pessoal Interno ☐ Acesso Pessoal Externo ☐ Outro ☐ _____	Sim ☐ Não ☐ N.A. ☐
Obs:			

ALOJAMENTO DADOS APLICAÇÃO (Storage)

Storage	Tipo storage	Consola de Gestão	Conformidade RGPD
Interno ☐	Dedicado ☐ Partilhado ☐ Em conjunto com a aplicação ☐ Cifrado ☐ Outro ☐ _____	Pessoal Interno ☐ Pessoal Externo ☐ Outro ☐ _____	Sim ☐ Não ☐ N.A. ☐
Externo ☐	Dedicado ☐ Partilhado ☐ Em conjunto com a aplicação ☐ Cifrado ☐ Outro ☐ _____	Pessoal Interno ☐ Pessoal Externo ☐ Outro ☐ _____	Sim ☐ Não ☐ N.A. ☐
Obs:			

BACKUPS DADOS PESSOAIS

Backups	**Tipo de backups**	**Backup e Reposição Testados**	**Implementado de acordo com o plano**
Interno ☐	Online ☐ Offline ☐ Outro ☐ _____	Sim ☐ Não ☐	Sim ☐ Não ☐
Externo ☐	Online ☐ Offline ☐ Outro ☐ _____	Sim ☐ Não ☐	Sim ☐ Não ☐
Obs:			

LOGGING E MONITORIZAÇÃO DE DADOS PESSOAIS

Controlo de acessos registado em log: Sim ☐ Não ☐

Log e formato (exemplo):

Existe monitorização sobre o log de controlo de acessos: Sim ☐ Não ☐

Alerta e destino:

Acesso (ler, alterar, remover) aos dados pessoais registado em log: Sim ☐ Não ☐

Log e formato (exemplo):

Existe monitorização sobre o acesso aos dados pessoais: Sim ☐ Não ☐

Alerta e destino:

Direitos exercidos pelos utilizadores guardados em log: Sim ☐ Não ☐

Acesso	**Log e formato (exemplo):**
Esquecimento	**Log e formato (exemplo):**
Atualização	**Log e formato (exemplo):**
Portabilidade	**Log e formato (exemplo):**
Outro: _____ _____	**Log e formato (exemplo):**

Existe monitorização sobre direitos exercidos pelos utilizadores dos dados pessoais: Sim ☐ Não ☐

Alerta e destino:

Verificação e auditoria de segurança (PII)
(Smoke testS PRD)

Os dados são filtrados consoante o perfil aplicacional? Sim ☐ Não ☐

Se sim, indique os tipos de filtros aplicados:

Filtros	Aplicado/Não Aplicado	Observação
Ofuscação	Sim ☐ Não ☐	
Anonimização	Sim ☐ Não ☐	
Outro: _____	Sim ☐ Não ☐	

É feito log dos acessos à aplicação? Sim ☐ Não ☐

Tipo de Log

É feito log dos direitos exercidos sobre os utilizadores? Sim ☐ Não ☐

Log dos direitos (exemplo):

Perante a reposição de um backup é garantido que não são repostos dados de utilizadores desatualizados, inexistentes à data? Sim ☐ Não ☐

Forma como é feita reposição de um backup:

Perante o ataque (exemplo: ransomware) os backups não são afetados? Sim ☐ Não ☐

Segurança dos backups dos dados pessoais:

Existe uma solução de DLP que monitoriza e controla o acesso aos dados pessoais? Sim ☐ Não ☐

Solução DLP (exemplo):

SOLUÇÃO DATA LOSS PREVENTION

Existe alguma solução de DLP afeta à aplicação: Sim ☐ Não ☐

Se sim, indique quais dos controlos foram ativados relativamente à aplicação:

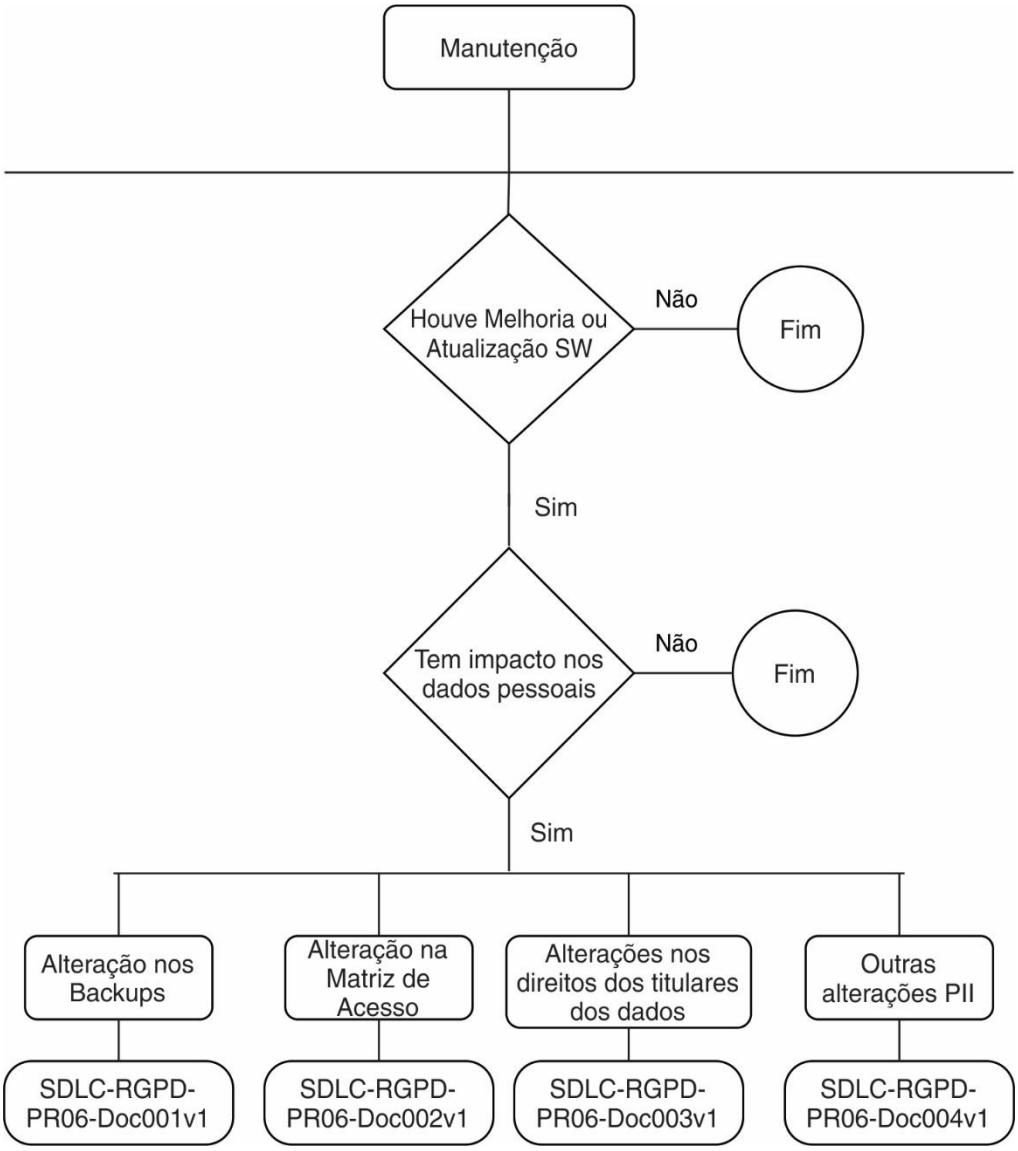
Controlo	Ativado?
Identificação de dados pessoais/sensíveis	Sim ☐ Não ☐
Classificação dos dados pessoais/sensíveis	Sim ☐ Não ☐
Monitorização das atividades que envolvem os dados pessoais/sensíveis	Sim ☐ Não ☐

Indique os tipos de monitorização cobertos pela solução de DLP:

Tipo monitorização	Controlos ativados
Data at rest	Restringir o acesso às funções administrativas locais, como a capacidade de instalar o software e modificar as configurações de segurança. Impedir malware, vírus, spyware, etc. Impedir a cópia de dados confidenciais em mídia não aprovada. Verificar se a extração autorizada de dados ocorre apenas na mídia criptografada.
Data in use	Monitorizar o acesso e o uso de dados de alto risco para identificar o uso potencialmente inadequado. Restringir as habilidades do usuário para copiar dados confidenciais em contêineres não aprovados (por exemplo, email, navegadores da Web), incluindo o controle da capacidade de copiar, colar e imprimir seções de documentos.
Data in motion	Impedir que dados confidenciais não criptografados deixem o perímetro. Registrar e monitorizar o tráfego de rede para identificar e investigar transferências inadequadas de dados sensíveis.

Monitorização ativa de Data Leaks	Verificar se o acesso remoto à rede da empresa está protegida e controlar os dados que podem ser salvos por meio de instalações remotas, como o Outlook Web Access

Procedimento 6 - Manutenção



Documentos de Especificação Manutenção:

MANUTENÇÃO **SDLC-RGPD-PR06-Doc001v1**
FASE SDLC - MANUTENÇÃO

1. OBJETIVO E ÂMBITO

Testes regulares à segurança aplicacional
e PII e após atualizações, gestão
de versões de aplicação e auditorias RGPD.
Cópias de segurança.
Verificar se houve alterações nos
backups que afetam a salvaguarda
das informações pessoais.

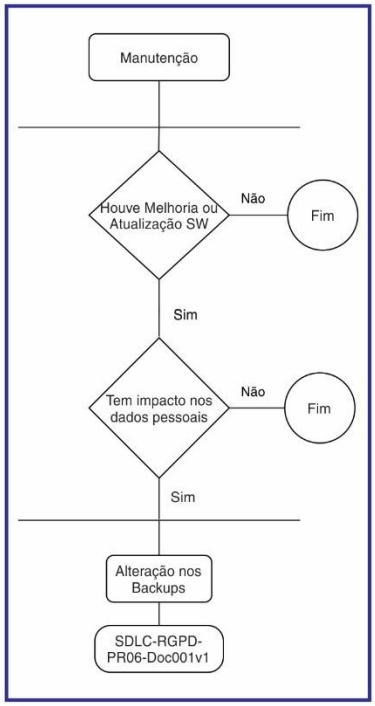
2. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

3. MODO DE PROCEDER

3.1 Documento de Manutenção: Doc001v1

3.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Verificar se houve melhoria ou atualização do software. Se não houve nenhuma alteração no software é o Fim do processo. Se houve melhoria ou atualização, verificar se tem impacto nos dados pessoais. Se as alterações não tiveram impacto nos dados pessoais é o Fim. Se houve impacto nos dados pessoais: No do documento Alteração nos Backups registar a data e o responsável pela alteração e as atualizações realizadas.	Equipa Manutenção Equipa Manutenção Equipa Manutenção	SDLC-RGPD-PR06-Doc.001V1.

Elaborado por: <Nome do Responsável pela Manutenção>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

4. OBJETIVO E ÂMBITO

Testes regulares à segurança aplicacional e PII e após atualizações, gestão de versões de aplicação e auditorias RGPD. Verificar se ocorreram alterações na matriz de acesso que afetam os dados pessoais.

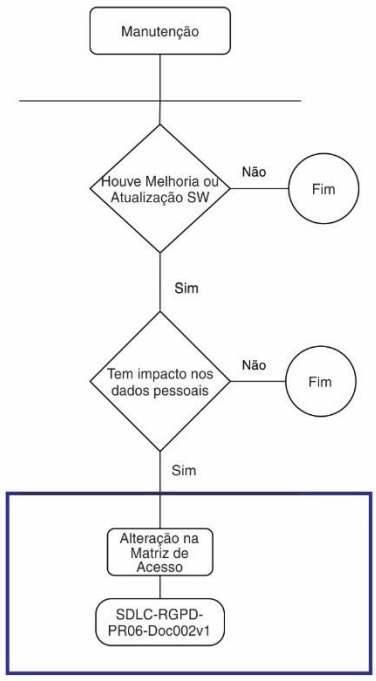
5. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

6. MODO DE PROCEDER

6.1 Documento de Manutenção: Doc002v1

6.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	No documento Alteração na Matriz de Acesso, registar apenas as alterações que afetam os dados pessoais, com a data que for realizada e o responsável pela alteração.	Equipa Manutenção	SDLC-RGPD-PR06-Doc.002V1.

Elaborado por: <Nome do Responsável pela Manutenção>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

7. OBJETIVO E ÂMBITO

Também dentre os documentos da Gestão de Configurações (PII), encontra-se o documento para fazer a verificação do Logging e monitorização de dados pessoais, garantindo o registro de acesso às PII.

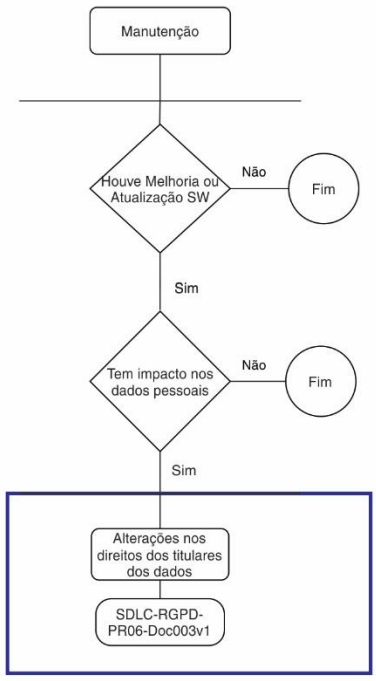
8. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

9. MODO DE PROCEDER

9.1 Documento de Manutenção: Doc003v1

9.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Registar no documento Alteração Direito dos Utilizadores as mudanças que afetam e causam impacto nos dados pessoais da aplicação.	Equipa Manutenção	SDLC-RGPD-PR06-Doc.003V1.

Elaborado por: <Nome do Responsável pela Manutenção>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

10. OBJETIVO E ÂMBITO

Após ser validado o teste controlo de acessos RGPD no documento da fase anterior, realizar a verificação e auditoria de segurança (PII) baseado no Smoke Test PRD, informando os tipos de filtro, log de acesso, log de direto, soluções DLP e backups, de segurança de acordo com o RGPD.

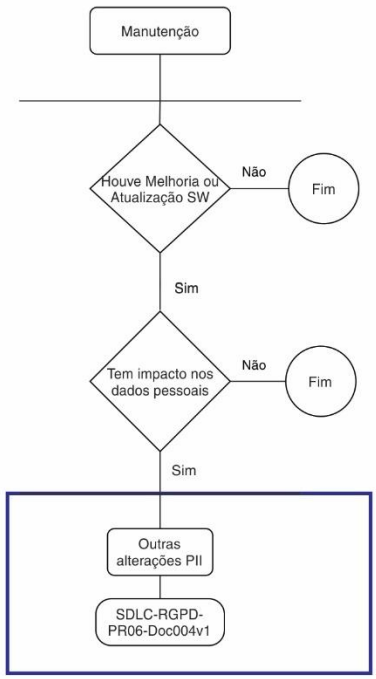
11. ABREVIATURAS E TERMOS

RGPD - Regulamento Geral de Proteção de Dados
SDLC - Ciclo de Desenvolvimento de Software
DPO - Responsável pelo tratamento dos dados
PII - Informação de Identificação Pessoal
Doc - Documento
v1 - Versão 1

12. MODO DE PROCEDER

12.1 Documento de Manutenção: Doc004v1

12.1.1 Documento Controlo SDLC - RGPD

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Registar no documento Outras Alterações PII e especificar qual alteração realizada e o conteúdo que afetará os dados pessoais no software.	Equipa Manutenção	SDLC-RGPD-PR06-Doc.004V1.

Elaborado por: <Nome do Responsável pela Manutenção>	Verificado por: <Nome do DPO>	Aprovado por: <Nome do Gestor de Projetos>
Data: <Ano-mês-dia>	Data: <Ano-mês-dia>	Data: <Ano-mês-dia>

ALTERAÇÃO NOS BACKUPS DOS DADOS PESSOAIS – DATA AT REST

1 – Alteração na informação recolhida da fase de análise e especificação de requisitos

Houve alterações nos backups que afetam a salvaguarda de dados pessoais: Sim ☐ Não ☐

Se SIM descreva alteração do plano de backups:

Tipo	Periodicidade	Tipo	Segurança	Local
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐
Outro		Offline ☐ Online ☐	Cifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐

Observações referente às alterações:

Data: ___ / ___ /_____ Nome: _____

ALTERAÇÃO NA MATRIZ DE ACESSOS / DADOS (DATA MAPPING)

Houve alterações nos backups que afetam a salvaguarda de dados pessoais: Sim ( ) Não ( )

Se SIM descreva alteração do plano de backups:

Data da alteração: ___/ ___/____ **Nome:**

INSTRUÇÕES: **SÓ DEVEM SER REGISTADAS AS ALTERAÇÕES!**
Especificar os campos da BD relativos às **alterações** dos dados pessoais/sensíveis na linha 6
Especificar **alterações** dos utilizadores/perfis na coluna A

Completar com S/N sendo "S" da **alteração** na indicação de operação permitida sobre os campos pelo utilizador/perfil e "N" a indicação de acesso proibido/desnecessário do utilizador/perfil correspondente

Função / Campo e Operações	Primeiro Nome				Sobrenome				Último nome				Telefone				Morada				Email				NIF				NISS				Género				Empresa				Tu
	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C
admin		S		S				S				S		S		S				S		S		S				S				S		S		S		S		S	
rh				S				S				S				S				S				S				S				S		S		S		N		N	
inf				S				N				N				N				N				N				N				N		S		S		N		N	
ana@xpto.com				N				N				N				N				N				N				N				N		S		S		S		S	
manuel@xpto.com				S				N				N				S				N				S				N				N		S		S		S		S	
DPO				S				S				S				S				N				S				S				S		S		S		S		S	

...				S				S				S				S				S				S				N				N		S		S		S		S		S		S		N		N		N		N		N		

ALTERAÇÃO DIREITOS DOS UTILIZADORES

Direito	Alterado	Formato	Observações das alterações
Acesso	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Portabilidade	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Esquecimento	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
Atualização	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	
	Sim ☐ Não ☐	Email ☐ Portal ☐ Formulário aplicacional ☐ Aviso ☐ Incluídos nos avisos legais ☐ Outro ☐	

Data: ___ / ___ /_____ Nome: _____

Outras alterações PII <Especificar>

Houve melhoria ou atualização do software? Sim ☐ Não ☐

Tem impacto nos dados pessoais? Sim ☐ Não ☐

Se ambos SIM indique:

Alteração <Especificar>	
Conteúdo	
Observações	

Se NÃO indique:

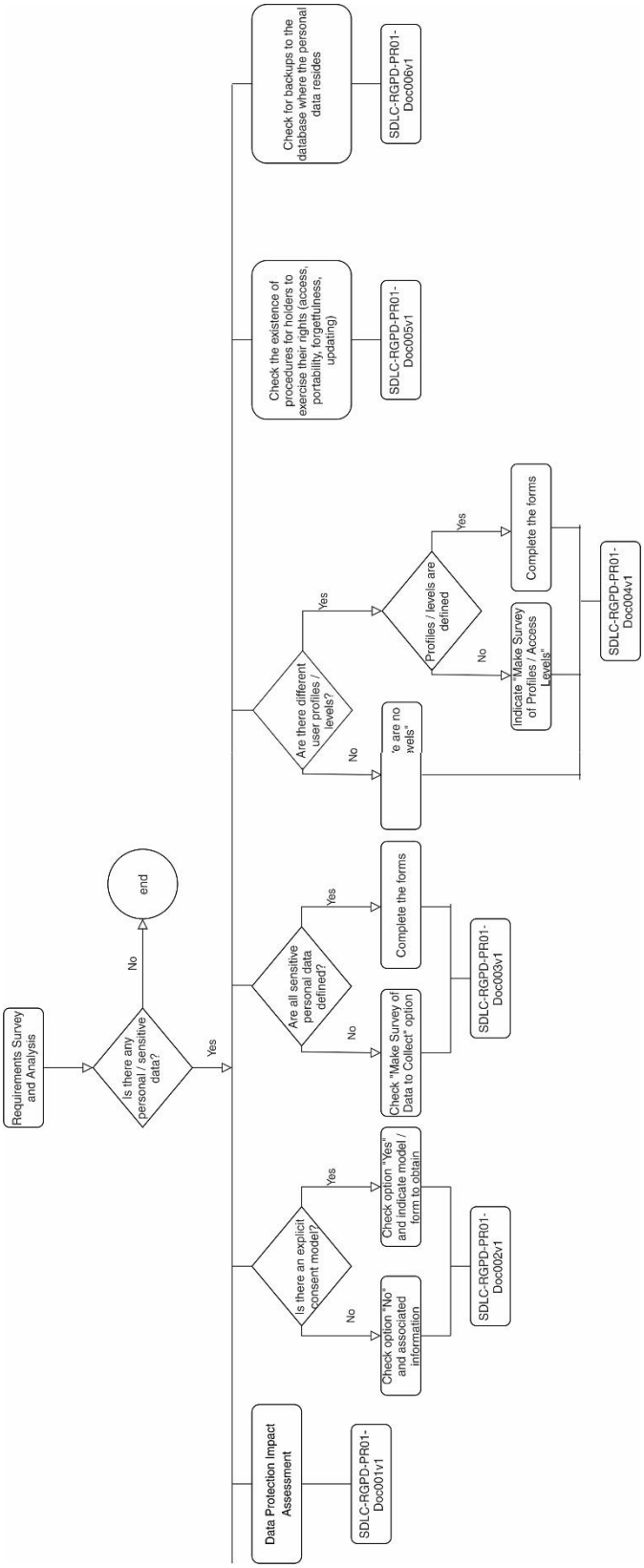
O que afeta as alterações no software?	
Especificar alterações	

Data: ___ / ___ /_____ Nome: _____

ATTACHMENT B - SDLC AND GDPR ALIGNMENT PROCESS

This document presents the alignment process between the SDLC and the GDPR. The process consists of six procedures. For each of the procedures, activities are presented with the flow of information and supporting documents, the procedure for each phase separated from flow to flow and with a description to make it clearer, as well as the models of each supporting document.

Procedure 1 - Requirements Analysis



Requirements Analysis Specification Documents:

SPECIFICATION OF PII SAFETY REQUIREMENTS **SDLC-RGPD-PR01-Doc001v1**
SDLC PHASE - REQUIREMENTS ANALYSIS

1. OBJETIVE AND SCOPE

Questionnaire document aiming to carry out the Impact Assessment on the protection of personal / sensitive data.

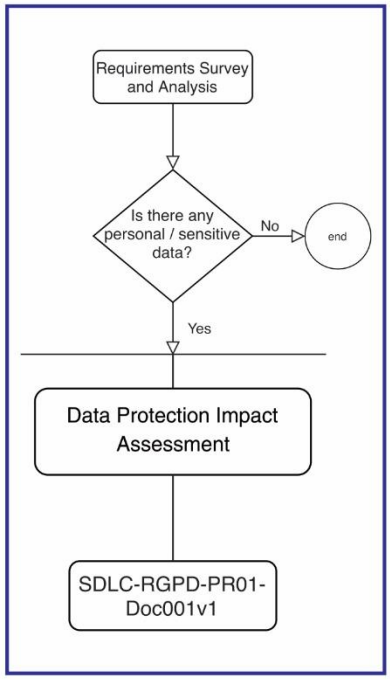
2. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

3. MODE OF PROCEDURE

3.1Requirements Document: Doc001v1

3.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Conduct the requirements survey and analysis and check if there will be personal / sensitive data in the application. If there is no personal / sensitive data, it is the End of the process. If so, carry out the impact assessment on the protection of personal / sensitive data that the application will use and determine the scope, objective, the team and managers, operations processing of personal data, carry out all document evaluations and predict security measures with recommendations improvements.	Sistems Analyst DPO	SDLC-RGPD-PR01-Doc.001V1.

Prepared by: <Sistems Analyst name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

4. OBJETIVE AND SCOPE

Questionnaire / interview
to determine if the application
makes use of personal / sensitive data.
Check if there is a model
explicit consent

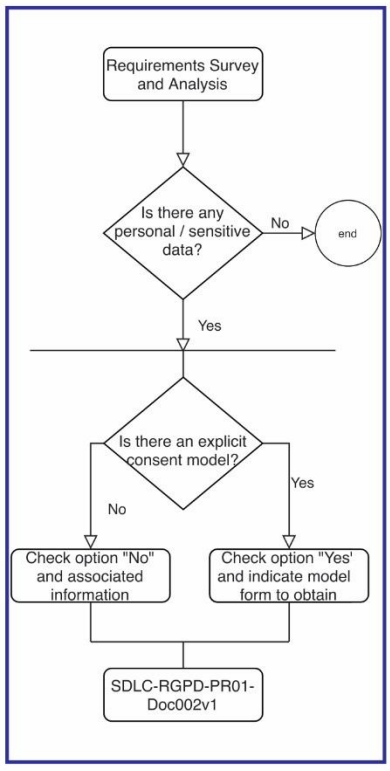
5. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

6. MODE OF PROCEDURE

6.1 Requirements document: Doc002v1

6.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	This procedure aims to collect information / specification of PII requirements. Check if the application makes use of personal data or sensitive data that can lead to the identification of a specific person? - First name; - Last name; - Full name; - Mobile number; - CC number; - Passport number; - Tax Identification Number; - Address; - Marital status; etc. • If there is no personal / sensitive data, it's the end of the diagram. • If yes, continue the analysis with the collection of others requirements below. Is there a model for requesting explicit consent? • If yes, provide the model indicated by registering this option in the CONSENT document. • If not, check that the consent form is appropriate for the request by adjusting the even if necessary.	Sistems Analyst Sistems Analyst Sistems Analyst Sistems Analyst	SDLC-RGPD-PR01-Doc.002V1.

Prepared by: <Sistems Analyst name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

7. OBJETIVE AND SCOPE

Questionnaire / interview to determine whether personal and sensitive data is defined and appropriate to the software project.

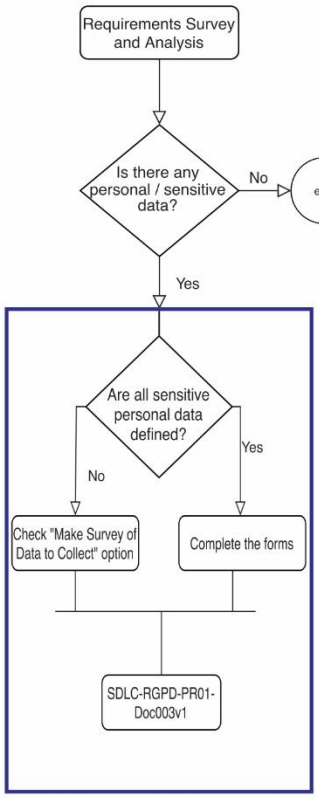
8. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

9. MODE OF PROCEDURE

9.1 DRequirements document: Doc003v1

9.1.1 DLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check if the model for indicating the personal and sensitive data to be collected and processed is suitable for the project. • If the data is already defined, you must complete the DATA-COLLECT Form. • If the personal data to be collected is not defined, you must make a survey to complete the DATA-COLLECT Form.	Sistems Analyst Sistems Analyst Sistems Analyst	SDLC-RGPD-PR01-Doc.003V1.

Prepared by: <Sistems Analyst name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

10. OBJETIVE AND SCOPE

Questionnaire / interview
to check if there are access levels / profiles in the application.

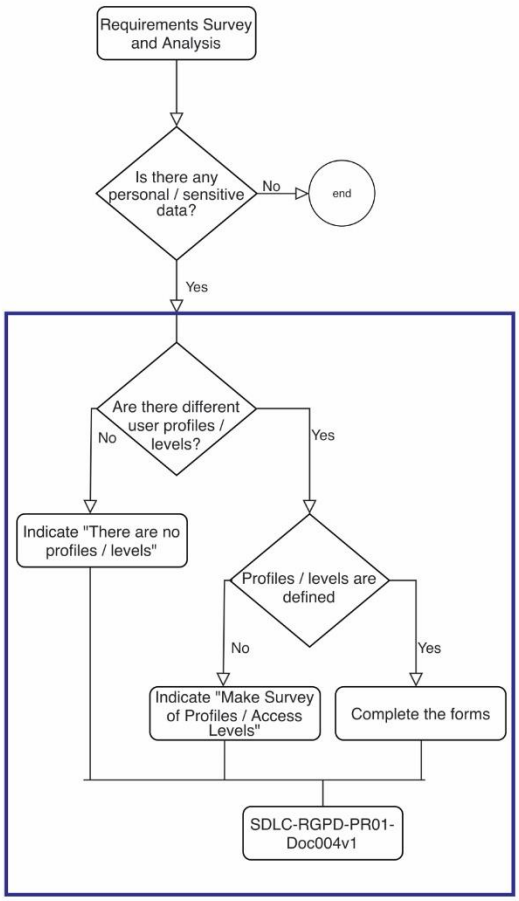
11. ABREVIATURAS E TERMOS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

12. MODE OF PROCEDURE

12.1 Requirements document: Doc004v1

12.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check if there are access levels / profiles in the application. • If there are no access levels / profiles in the application, you must indicate this in the PROFILES document. • If there are access levels / profiles in the application, and if they are already defined, then you must complete the PROFILES document. • If they are not defined, you must make a survey to complete the PROFILES document.	Sistems Analyst Sistems Analyst Sistems Analyst Sistems Analyst	SDLC-RGPD-PR01-Doc.004V1.

Prepared by: <Sistems Analyst name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

13. OBJETIVE AND SCOPE

Questionnaire / interview to verify the access participation of the holders of personal data about your access rights and orders.

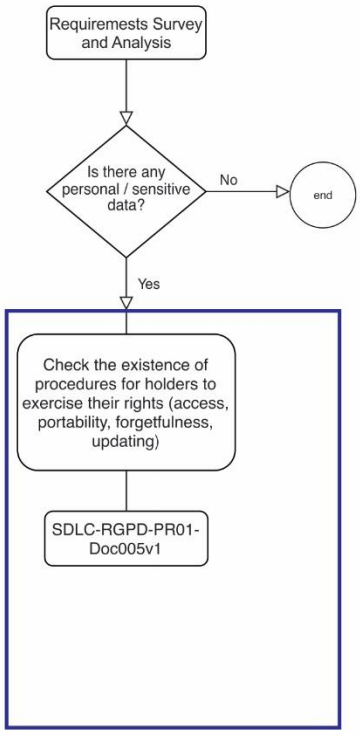
14. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

15. MODE OF PROCEDURE

15.1 Requirements document: Doc005v1

15.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check how the access of personal data holders will be in relation to their rights: • Right of access to personal data; • Portability requests; • Requests for forgetting personal data; • Update of personal data. Record the options in the RIGHTS-HOLDER-DATA form.	Sistems Analyst Sistems Analyst	SDLC-RGPD-PR01-Doc.005V1.

Prepared by: <Sistems Analyst name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

16. OBJETIVE AND SCOPE

Questionnaire / interview to
check if DB backups are included
where they appear
personal data for the application.

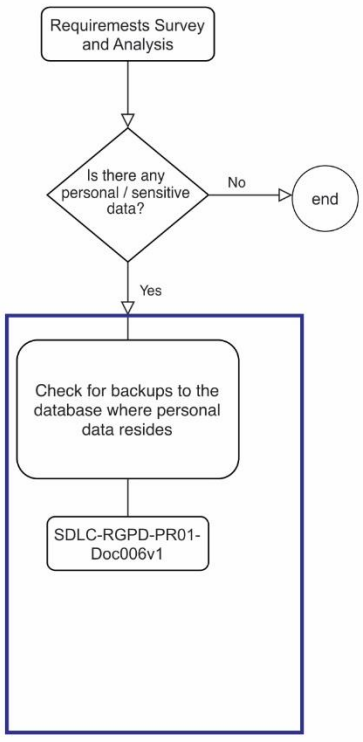
17. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1
BD - Data Base

18. MODE OF PROCEDURE

18.1 Requirements document: Doc006v1

18.1.1 SDLC Control Document - GDPR

ATIVIDADES	DESCRIÇÃO	RESP.	DOC.
	Check if backups of the database are included where personal data are included. • If included, the plan must be presented in the BACKUPS document. • If the issue is not reflected in the BACKUPS document with an indication of the procedure to be followed.	Sistems Analyst Sistems Analyst Sistems Analyst	SDLC-RGPD-PR01-Doc.006V1.

Prepared by: <Sistems Analyst name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

1 - Scope of the DPIA:

2 - Purpose of impact assessment:

3 - Team and contacts of those responsible, indicate:

Name	Contact

---

4 - Personal Data Processing Operations:

Context and purpose of the processing of personal data	
Important assets that depend on personal data (components, systems, networks, role)	
Access to personal data	< It will be handled by the process identified in the document SDLC-RGPD-PR01-Doc004v1>
Description of personal data processing operations	< It will be handled by the process identified in the document SDLC-RGPD-PR01-Doc003v1>

---

5 - Assessment of needs in processing operations:

Measures planned to demonstrate compliance and need for treatment	

Measures that contribute to the rights of data subjects	<It will be handled by the process identified in the document SDLC-RGPD-PR01-Doc005v1>

---

6 - Assess and mitigate risks inherent in data subjects' rights:

Related to breach of confidentiality or integrity	
Related to the loss of personal data	
Related to the exercise of data subjects rights	<Process identified in the User Rights document SDLC-RGPD-PR01-Doc005v1 >
Possible impacts and threats	
Risk reduction measures with technical descriptions	

---

7 – Provide for security measures and procedures to ensure data protection:

Indicate:

Description of technical measures to ensure protection	<Process identified in the Personal Data Backups document SDLC-RGPD-PR01-Doc005v1. Other technical solutions are included in the maintenance documents SDLC-RGPD-PR05-Doc001v1, SDLC-RGPD-PR05-Doc002v1, SDLC-RGPD-PR05-Doc003v1, SDLC-RGPD-PR05-Doc004v1, SDLC-RGPD-PR05-Doc005v1>

8 – Improvement recommendations:

CONSENT, PRIVACY AND TERMS & CONDITIONS

Is the safeguarding of the registration date / time of consent contemplated? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

Is there an explicit consent model? Yes ☐ No ☐

If YES indicate:

How to get	
Can be used without adaptation	Yes ☐ No ☐
Adaptation to be made	

If NO indicate:

Delegate in the drawing phase	Yes ☐ No ☐
Content	

Is there a model of privacy policy? Yes ☐ No ☐

If YES indicate:

How to get	
Can be used without adaptation	Yes ☐ No ☐
Adaptation to be made	

If NO indicate:

Delegate in the drawing phase	Yes ☐ No ☐
Content	

Is there model terms and conditions? Yes ☐ No ☐

If YES indicate:

How to get	
Can be used without adaptation	Yes ☐ No ☐
Adaptation to be made	

If NO indicate:

Delegate at the design stage	Yes ☐ No ☐
Content	

DATA COLLLECTION AND PROCESSING – DATA SPECIFICATION

Personal / sensitive data and collect and process

Field	Collect Y/N?	Justification
First Name	Yes ☐ No ☐ to be defined ☐	
Last Name	Yes ☐ No ☐ to be defined ☐	
Full Name	Yes ☐ No ☐ to be defined ☐	
Number Phone	Yes ☐ No ☐ to be defined ☐	
CC Number	Yes ☐ No ☐ to be defined ☐	
Passport Number	Yes ☐ No ☐ to be defined ☐	
Tax Identification Number	Yes ☐ No ☐ to be defined ☐	
Address	Yes ☐ No ☐ to be defined ☐	
Political Affiliation	Yes ☐ No ☐ to be defined ☐	
Religion	Yes ☐ No ☐ to be defined ☐	
Diseases	Yes ☐ No ☐ to be defined ☐	
Age	Yes ☐ No ☐ to be defined ☐	
Genre	Yes ☐ No ☐ to be defined ☐	
Email	Yes ☐ No ☐ to be defined ☐	
Birth Date	Yes ☐ No ☐ to be defined ☐	
...	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	

	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	
	Yes ☐ No ☐ to be defined ☐	

PROFILES / LEVELS ACESS CONTROL

There are different levels / profiles of application / data access: Yes ☐ No ☐

If YES, indicate the profiles / application levels

Profile	Acess level	Observation
Admin	Unlimited ☐ Limited ☐ to be defined ☐	
...

RIGHTS OF USERS

Is the safeguarding of the registration date / time of consent contemplated? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____________

Right	State	Format	Comments
Acess	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
Portability	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
Forgetfulness	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
Update	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐	

		Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	
	Support already ☐ To create ☐ not necessary ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in the legal notices ☐ Other ☐	

BACKUPS OF PERSONAL DATA – DATA AT REST

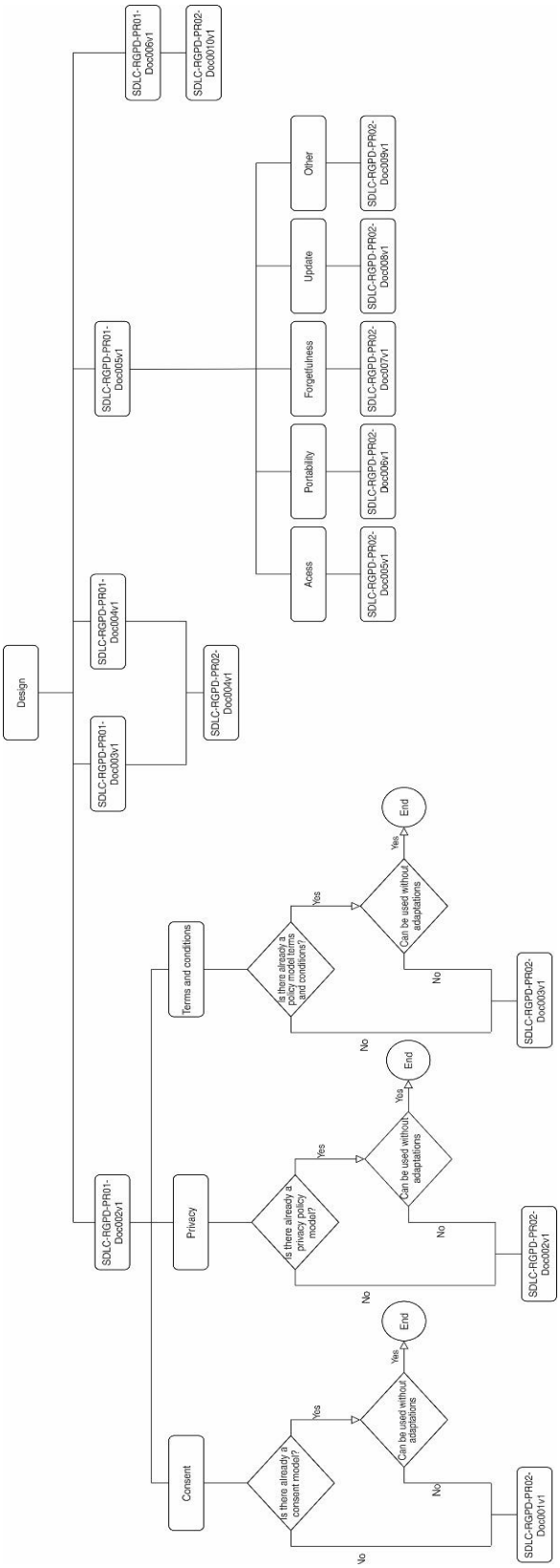
Backup policies exist in the organization: Yes ☐ No ☐ N.A. ☐

Backups of the data to be created within the application must be made: Yes ☐ No ☐

If YES describe the backup plan:

Type	Frequency	Type	Safety	Local
Total	Diary ☐ Weekly ☐ Monthly ☐ Other _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Incremental	Diary ☐ Weekly ☐ Monthly ☐ Other _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Archive logs	Size _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Other		Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐

Procedure 2 - Design



Specification Documents Design:

DESIGN **SDLC-RGPD-PR02-Doc001v1**

SDLC PHASE - DESIGN

1. OBJETIVE AND SCOPE

Include in software design
aspects related to the GDPR
namely consent,
of the holder of personal data
regarding the use of their PII.

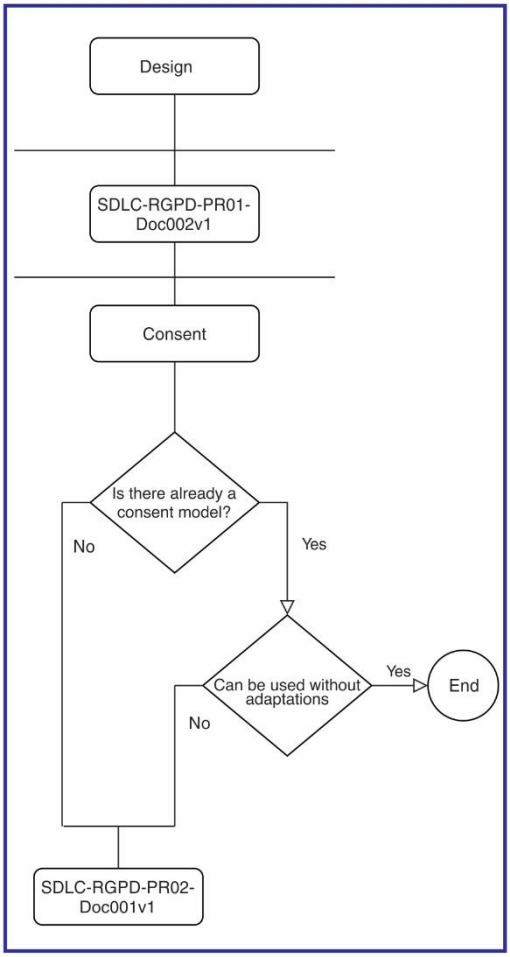
2. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

3. MODE OF PROCEDURE

3.1 Design Document: Doc001v1

3.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	In the design phase of the SDLC, include the GDPR according to the information collected in the requirements analysis of the first stage of development document software SDLC-RGPD-PR01-Doc001v1. Abrir no Google Tradutor CONSENT Check if there is already a model consent. • If there is no consent, complete the CONSENT document. • If the model exists consent: Check that it can be used without adaptations. • If so, it is the end. • If not, complete the document of consent.	Designer Designer Designer Designer Designer Designer	SDLC-RGPD-PR02-Doc.001V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

4. OBJETIVE AND SCOPE

Include in software design aspects related to the GDPR namely privacy personal data of the holder of personal data

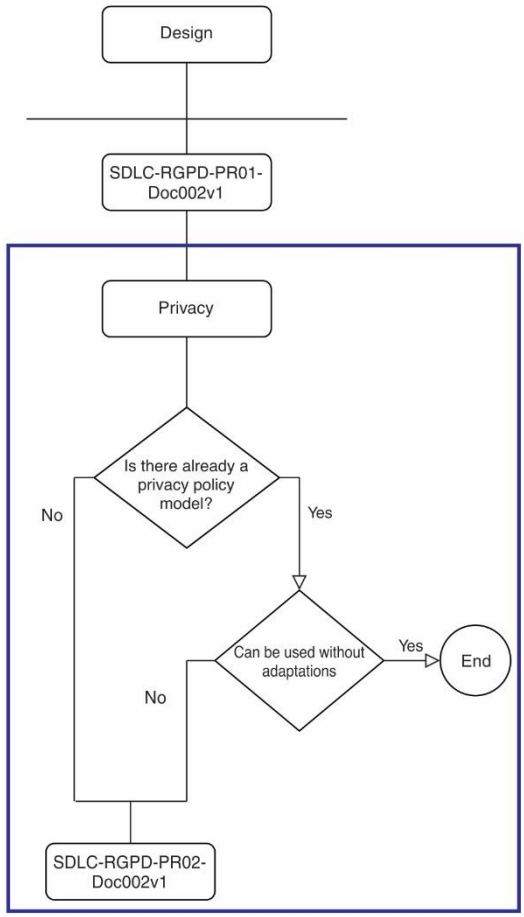
5. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

6. MODE OF PROCEDURE

6.1 Design Document: Doc002v1

6.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	PRIVACY Check if there is already a model privacy policy. • If there is no privacy policy, fill in the PRIVACY document. • If theprivacy policy, check if it can be used without adaptations. • If so, then it's the end. • If not, complete the document privacy.	Designer Designer Designer Designer Designer	SDLC-RGPD-PR02-Doc.002V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

7. OBJETIVE AND SCOPE

Include in software design aspects related to the GDPR namely Terms and Conditions for use of the holder's personal data of PII.

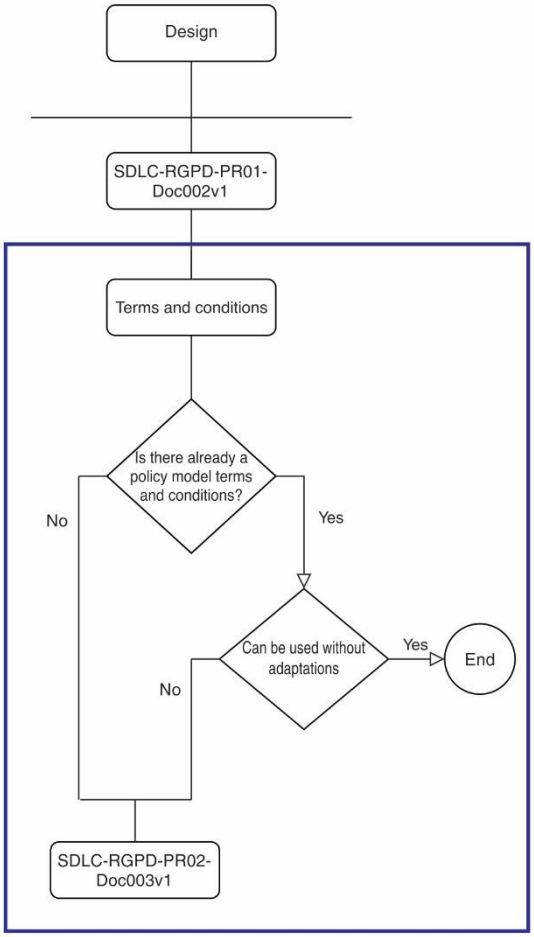
8. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

9. MODE OF PROCEDURE

9.1 Design Document: Doc003v1

9.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	TERMS AND CONDITIONS Check if there is already a model terms and conditions policy • If there is no terms and conditions policy, you must complete the document TERMS AND CONDITIONS. • If yes, check if it can be used without adaptations. • If so, then it's the end. • If not, fill in the TERMS AND CONDITIONS	Designer Designer Designer Designer Designer	SDLC-RGPD-PR02-Doc.003V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

10. OBJETIVE AND SCOPE

Specify the existing application profiles, what data is required to be collected by users, where the data will be stored, (matrix).

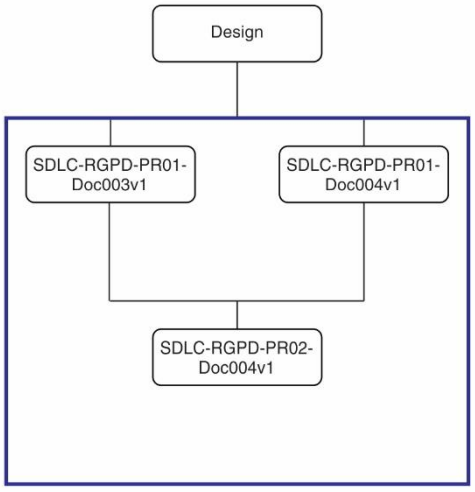
11. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

12. MODE OF PROCEDURE

12.1 Design Document: Doc004v1

12.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check that the document DATA COLLECTION AND TREATMENT - DATA SPECIFICATION (SDLC-RGPD-PR01-Doc003v1) and the document PROFILES / LEVELS ACCESS CONTROL (SDLC-RGPD-PR01-Doc004v1) are defined. • If both documents are defined, then fill in the matrix of the document DATA MAPPING.	Designer Designer	SDLC-RGPD-PR02-Doc.004V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

13. OBJETIVE AND SCOPE

Add to the software design aspects related to the GDPR of Right of Access to personal data by the data subject, after defining users' rights according to requirements analysis.

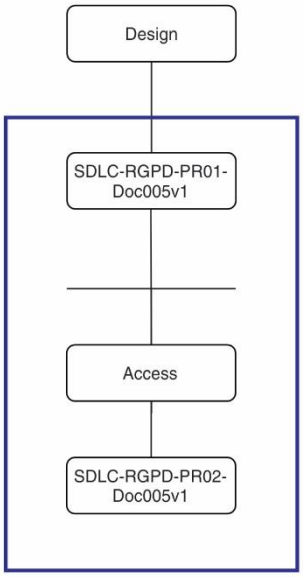
14. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

15. MODE OF PROCEDURE

15.1 Design Document: Doc005v1

15.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check if the document RIGHT-HOLDERS-DATA (SDLC-RGPD-PR01-Doc005v1) is defined. ACCESS • Fill out the PII HOLDER ACCESS RIGHTS document, defining the format, design / mockup / description.	Designer Designer	SDLC-RGPD-PR02-Doc.005V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

16. OBJETIVE AND SCOPE

Contain in the software design aspects related to the GDPR of Personal data portability right the PII, after defining the users' rights according to requirements analysis.

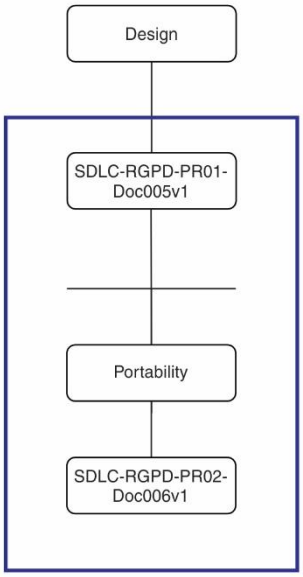
17. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

18. MODE OF PROCEDURE

18.1 Design Document: Doc006v1

18.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check if the document RIGHT-HOLDERS-DATA (SDLC-RGPD-PR01-Doc005v1) is defined. PORTABILITY • Fill out the PII HOLDERS 'PORTABILITY RIGHTS document, defining the format, design / mockup / description.nsla	Designer Designer	SDLC-RGPD-PR02-Doc.006V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

19. OBJETIVE AND SCOPE

Contain in the software design aspects related to the GDPR of forgetting personal data the data subject, after defining users' rights according to requirements analysis.

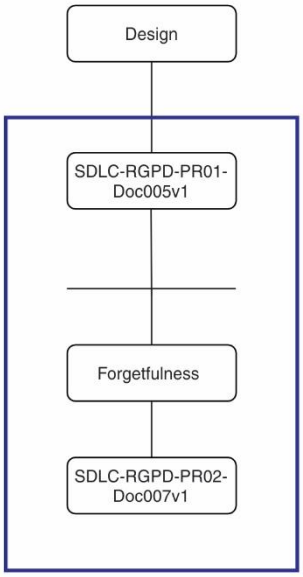
20. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

21. MODE OF PROCEDURE

21.1 Design Document: Doc008v1

21.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check if the document RIGHT-HOLDERS-DATA (SDLC-RGPD-PR01-Doc005v1) is defined. FORGETFULNESS • Complete the PII FORGETTING RIGHTS document, defining the format, design / mockup / description.	Designer Designer	SDLC-RGPD-PR02-Doc.007V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

22. OBJETIVE AND SCOPE

Add to the software design aspects related to the GDPR of the updating of personal data the data subject, after defining users' rights according to requirements analysis.

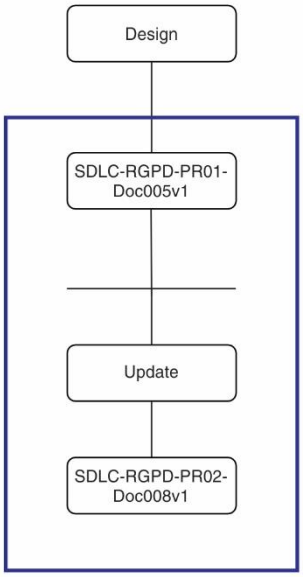
23. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

24. MODE OF PROCEDURE

24.1 Design Document: Doc007v1

24.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check if the document RIGHT-HOLDERS-DATA (SDLC-RGPD-PR01-Doc005v1) is defined. UPDATE • Complete the PII UPDATE document, defining the format, design / mockup / description.	Designer Designer	SDLC-RGPD-PR02-Doc.008V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

25. OBJETIVE AND SCOPE

Add to the software design aspects related to the GDPR, regarding the other type of right requested by the data subject, after defining users' rights according to requirements analysis.

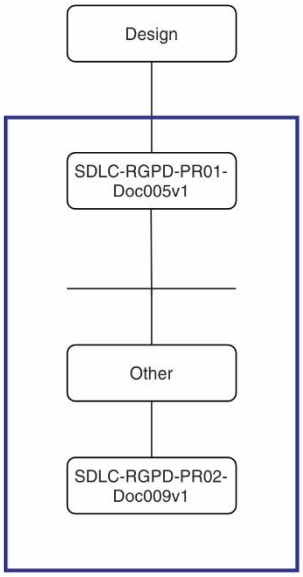
26. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

27. MODE OF PROCEDURE

27.1 Design Document: Doc009v1

27.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check if the document RIGHT-HOLDERS-DATA (SDLC-RGPD-PR01-Doc005v1) is defined. OTHER • Fill in the PII HOLDER RIGHTS document, specify the other right required by the data subject, defining the format, design / mockup / description.	Designer Designer	SDLC-RGPD-PR02-Doc.009V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

28. OBJETIVE AND SCOPE

Specify profiles existing application systems that data are needed to collect by users, where the data will be stored, (matrix).

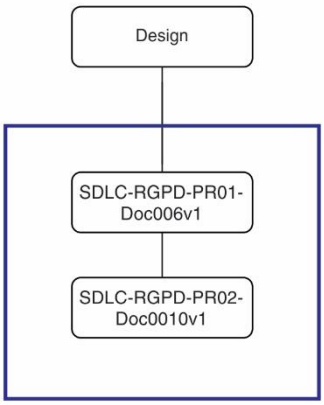
29. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

30. PROCEDURE

30.1 Design Document: Doc0010v1

30.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check if the documents BACKUPS OF PERSONAL DATA - DATA AT REST (SDLC-RGPD-PR01-Doc006v1) are defined. Validate the PERSONAL DATA BACKUPS Information - DATA AT REST and indication for the following phases.	Designer Designer	SDLC-RGPD-PR02-Doc.0010V1.

Prepared by: <Designer name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

CONSENT

Is the safeguarding of the registration date / time of consent contemplated? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

Is there an explicit?	Yes ☐	No ☐
Can be used without adaptations?	Yes ☐	No ☐

Text/drawing of the form / page to be created

[Design/Mockup]

PRIVACY

Is the safeguarding of the registration date / time of privacy contemplated? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

Is there model a privacy policy?	Yes ☐	No ☐
Can be used without adaptations?	Yes ☐	No ☐

Text/drawing of the form / page to be created

[Drawing/Mockup]

TERMS & CONDITIONS

Is the safeguarding of the registration date / time of terms and conditions contemplated?
Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

Is there model terms and conditions?	Yes ☐	No ☐
Can it be used without adaptations?	Yes ☐	No ☐

Text/drawing of the form / page to be created

[Design/Mockup]

ACESS MATRIX / DATA (DATA MAPPING)

INSTRUCTIONS:
Specify the DB fields for personal / sensitive data in line 6
Specify users profiles in column A

Complete with Y/N with "Y" indicating the de access allowed to the fields by the user / profiles and "N" indicating the prohibited / unnecessary access of the corresponding user / profile

User/Role / Field	First name	Second name	First name	Telphone	Adress	Email	NIF	NISS	Genrer	Company	Shift	Data Saída	Locality	Education	Civil Status	Login	Acess Type	Password	Level	Qualifcations	...	...
admin	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	N	S	S		
rh	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	N	S	S		
inf	S	N	S	N	N	N	N	N	S	N	N	N	N	N	N	N	N	N	N	N		
ana@xpto.com	N	N	N	N	N	N	N	N	S	N	N	N	N	N	N	N	N	N	N	N		
manuel@xpto.com	S	N	N	S	N	S	N	N	S	S	S	N	N	N	N	N	N	N	N	N		
DPO	S	S	S	S	N	S	S	S	S	S	S	N	S	S	S	S	S	N	S	S		
...	S	S	S	S	S	S	N	N	S	S	S	N	N	N	N	N	N	N	N	N		
...																						

RIGHTS OF PII HOLDERS – **ACCESS**

Is the safeguarding of the registration date / time of acess? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

State
Support already exists ☐ to create ☐ not necessary ☐

Format		**Design/Mockup/Description**
Email	☐	<Indicate the email address through which users can request access to your PII. Indicate whether to include the existence of that email address in any location of the application (Menu | terms and conditions | privacy | ...). The email may also be designed / specified for that purpose.>
Portal	☐	<Indicate if the company portal / website already exists through which users can make a request for access to their PII. Indicate if it is to include the existence of that portal / site somewhere in the application (Menu | terms and conditions privacy| ...)>
Application form	☐	<Design/specify the application form to be included in the application that allows data holders to request to their PII through it.>
Warning	☐	<Specify the warning (page) to be presented to users who wish to make a request for access to their PII or how the programmer should fit this request in the application.>
Included in legal warning	☐	<This case applies when the way of making a request for access to the PII is included in the legal warning and it can also be described how the programmer should fit it in the application>
Other _____ _____	☐	

_____		

RIGHTS OF PII HOLDERS – **PORTABILITY**

Is the safeguarding of the registration date / time of portability? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

State
Support already exists ☐ to create ☐ not necessary ☐

Format		**Design/Mockup/Description**
Email	☐	<Indicate the email address through which users can make a request for data portability. Indicate whether to include the existence of that email address somewhere in the application (Menu | terms and conditions | privacy | ...). The email may also be designed / specified for that purpose.>
Portal	☐	<Indicate, if it already exists, the company portal / website through which users can make a request for data portability. Indicate whether to include the existence of that portal / site in any location of the application (Menu | terms and conditions | privacy) ...)>
Aplicacional form	☐	<Design / specify the application form to be included in the application that allows data holders to make a PII portability request through it. >
Warning	☐	<Specify the warning (page) to present users who want to make a PII portability request or how the programmer should fit this request in the application.>
Included in legal notices	☐	<This case applies when the way of making a request for data portability is included in the legal notices and the way in which the programmer should fit this into the application can also be described.>
Other _____ _____	☐	

_____		

RIGHTS OF PII HOLDERS – **FORGETTING**

Is the safeguarding of the registration date / time of forgetting? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

State
Support already exists ☐ to create ☐ not necessary ☐

Format		**Design/Mockup/Description**
Email	☐	<Indicate the email address through which users can make a request for forgetting your PII. Indicate whether to include the existence of that email address somewhere in the application (Menu | terms and conditions | privacy | ...). The email may also be designed / specified for the purpose.>
Portal	☐	<Indicate if the company portal / website already exists through which users can make a request to forget their PII. Indicate whether to include the existence of that portal / site in any location of the application (Menu | terms and conditions | privacy | ...)>
Application form	☐	< Design / specify the application form to be included in the application that allows data holders to make a request to forget their PII>
Warning	☐	<Specify the warning (page) to present to users who wish to make a request to forget their PII or how the programmer should fit that request into the application >
Included in legal notices	☐	< This case applies when the way of making a request for forgetting the PII is included in the legal notices and it can also be described how the programmer should fit this in the application >
Other _____ _____	☐	

_____		

RIGHTS OF PII HOLDERS – **UPDATE**

Is the safeguarding of the registration date / time of update? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

State
There is already support ☐ to create ☐ not necessary ☐

Format		**Design/Mockup/Description**
Email	☐	<Indicate the email address through which users can make a request to update their PII. Indicate whether to include the existence of that email address in any location of the application (Menu | terms and conditions | privacy | ...). The email may also be designed / specified for the purpose.>
Portal	☐	< Indicate if the company portal / website already exists through which users can make a request to update their PII. Indicate whether to include the existence of that portal / site in any location of the application (Menu | terms and conditions | privacy | ...)>
Application form	☐	< Design / specify the application form to be included in the application that allows data holders to make a request to update their data >
Warning	☐	<Specify the warning (page) to display users who want to make a request to update their PII or how the developer should fit that request in the application
Included in legal notices	☐	< This case applies when the way to make a request to update the PII is included in the legal notices and it can also be described how the programmer should fit it in the application >
Other _____ _____ _____	☐	

RIGHTS OF PII HOLDERS – **<SPECIFY>**

Is the safeguarding of the registration date / time? Yes ☐ No ☐

What form? ☐ Database ☐ Email ☐ Application specifies GDPR ☐ Other_____

State
There is already support ☐ to create ☐ not necessary ☐

Format		**Design/Mockup/Description**
Email	☐	
Portal	☐	
Application form	☐	
Warning	☐	
Included in legal notices	☐	
Other _____ _____ _____	☐	

BACKUPS OF PERSONAL DATA – DATA AT REST

1 - Information collected from the requirements specification and analysis phase

Are there backup policies in the organization: Yes ☐ No ☐ N.A. ☐

Should the data to be created within the application be backup: Yes ☐ No ☐

If YES, describe the backup plan:

Type	Frequency	Type	Safety	Local
Total	Diary ☐ Weekly ☐ Monthly ☐ Other _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Incremental	Diary ☐ Weekly ☐ Monthly ☐ Other _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Archive logs	Size _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Other		Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐

2 – Information validation and indication for the following phases

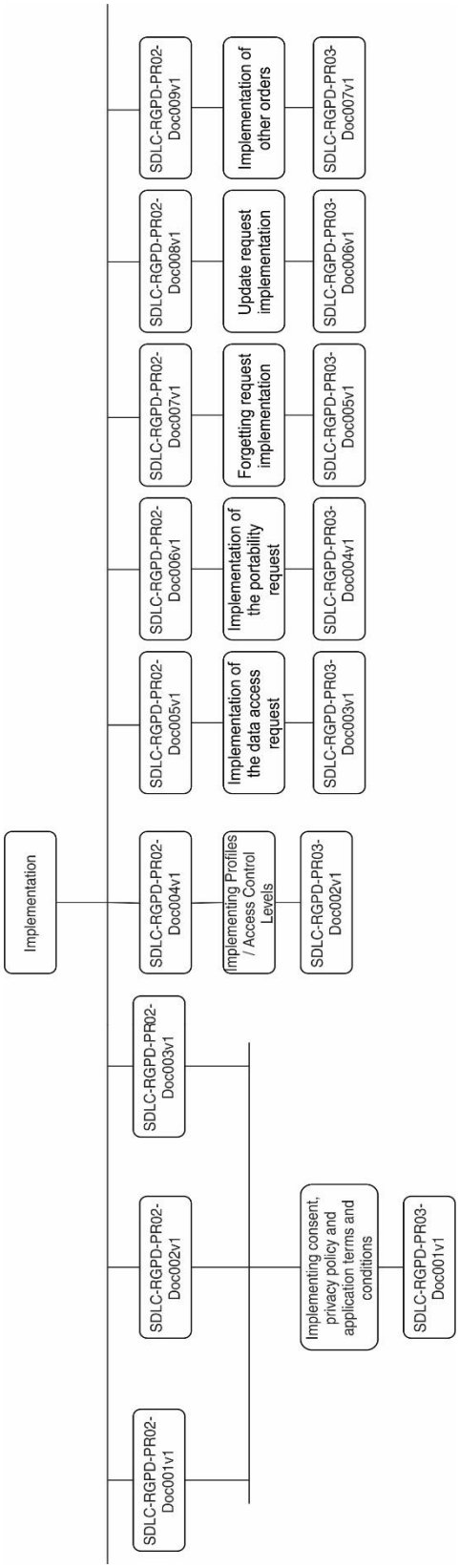
Do I validate information regarding backups: Yes ☐ No ☐

Backups plan (s) to implement:

Type	Frequency	Type	Safety	Local	Impl
Total	Diário ☐ Semanal ☐ Mensal ☐ Outro ____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
Incremental	Diário ☐ Semanal ☐ Mensal ☐ Outro ____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
Archive logs	Tamanho _____	Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐
...		Offline ☐ Online ☐	Crifrados ☐ Não Cifrados ☐	Onsite ☐ Offsite ☐	☐

Observations:

Procedure 3 - Implementation



Specification Documents Implementation:

1. OBJETIVE AND SCOPE

Software coding according to the GDPR principles (identified in the design phase).
Implement the application consent models, privacy, terms and conditions application.

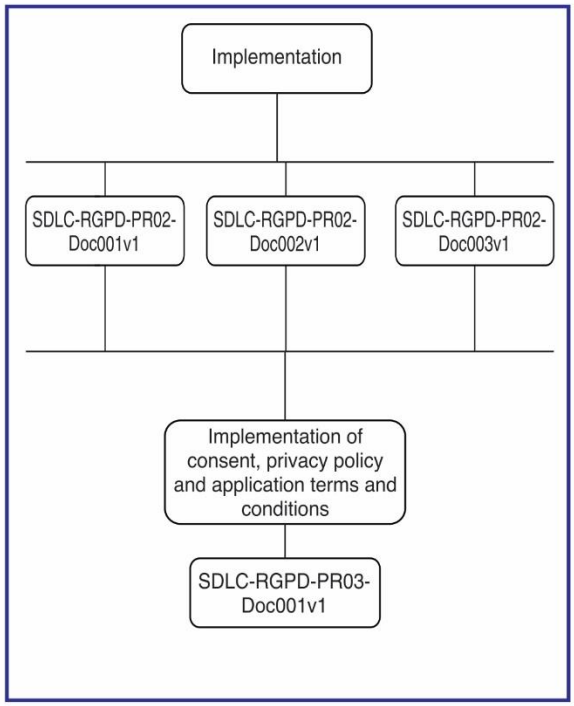
2. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

3. MODE OF PROCEDURE

3.1 Implementation Document: Doc001v1

3.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	At the Implementation stage SDLC, include the GDPR in coding the software according to the information collected at the design stage, with the documents defined in previous phase. According to the document consent, policy of privacy and terms and application conditions. Implement the templates in the application of consent privacy, terms and application conditions and indicate in the document Consent, Privacy, Terms & Conditions the form how was each implemented one of the models (Web page and link, Form, Email, Final template or other).	Developer Developer Developer	SDLC-RGPD-PR03-Doc.001V1.

Prepared by: <Developer Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

4. OBJETIVE AND SCOPE

Follow the parent document of design phase and implement access control considering profiles and data access. Consider the storage location data with strong cipher.

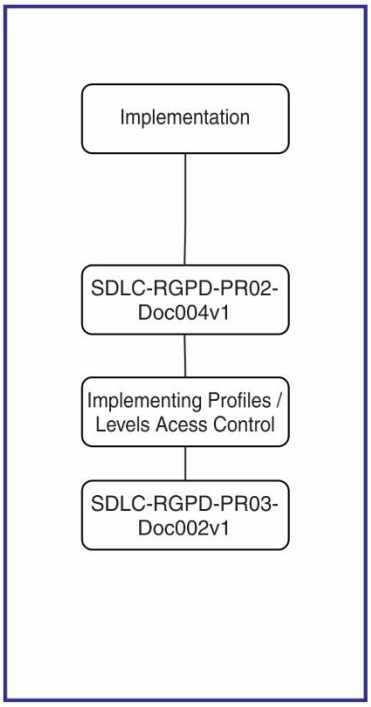
5. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

6. MODE OF PROCEDURE

6.1 Implementation Document: Doc002v1

6.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	According to the document Access / Data (Data Mapping), implemented menting Data Access Control Personal. Specify in the Access Control document Personal Data Profiles / Levels Control Access that have been implemented according to the Access Matrix of the design and inform whether the database is or not protected with encryption mechanisms and which control adopted for the user / profile and BD field.	Developer Developer	SDLC-RGPD-PR03-Doc.002V1.

Prepared by: <Developer Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

7. OBJETIVE AND SCOPE

Implementation of the right to access to personal data by users, following the document of the design phase SDLC-RGPD-PR02-Doc005v1

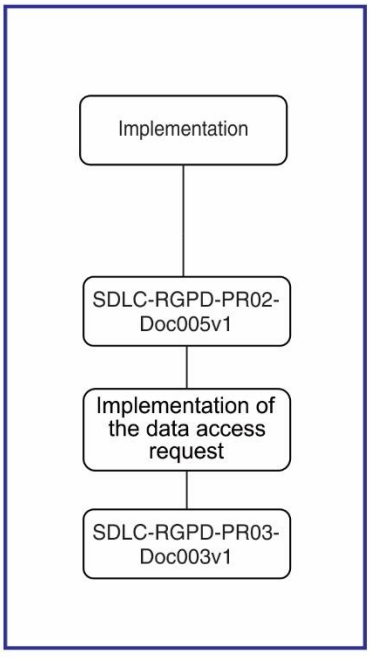
8. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

9. MODE OF PROCEDURE

9.1 Implementation Document: Doc003v1

9.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Follow the phase document drawing RIGHTS OF PII HOLDERS - ACCESS. Fill document Order implementation access to personal data. If implemented, indicate the form that was used. If it has not been implemented, indicate the reason.	Developer Developer Developer Developer	SDLC-RGPD-PR03-Doc.003V1.

Prepared by: <Developer Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

10. OBJETIVE AND SCOPE

Implementation of the right to portability of personal data by users, following the document of the drawing phase SDLC-RGPD-PR02-Doc006v1

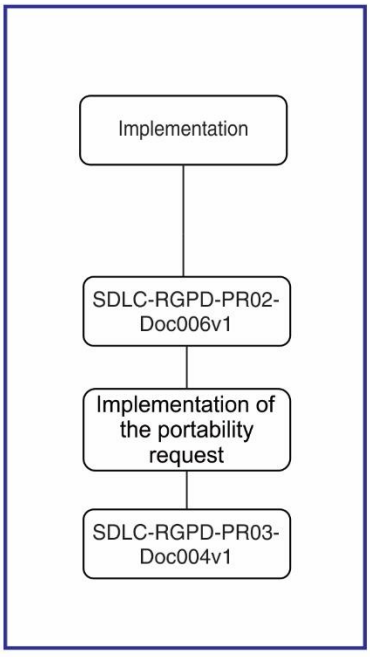
11. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

12. MODE OF PROCEDURE

12.1 Implementation Document: Doc004v1

12.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Follow the phase document drawing RIGHTS OF PII HOLDERS - PORTABILITY. Fill document Order implementation data portability personal. If implemented, indicate the form that was used. If it has not been implemented, indicate the reason.	Developer Developer Developer Developer	SDLC-RGPD-PR03-Doc.004V1.

Prepared by: <Developer Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

13. OBJETIVE AND SCOPE

Implementation of the right to forgetting personal data by users, following the document of the design phase SDLC-RGPD-PR02-Doc005v1

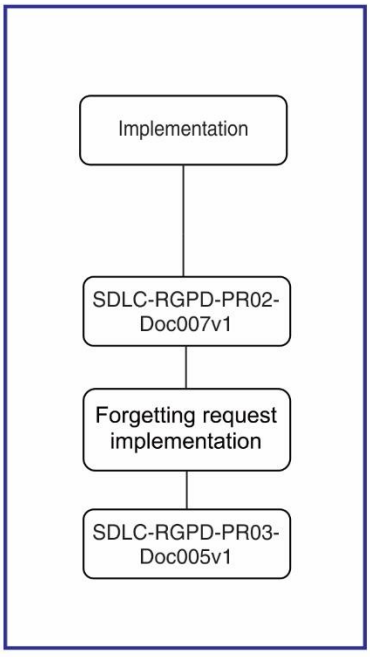
14. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

15. MODE OF PROCEDURE

15.1 Implementation Document: Doc005v1

15.1.1 Documento Controlo SDLC - RGPD

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Follow the phase document drawing RIGHTS OF PII HOLDERS - FORGETTING. Fill document Order implementation forgetfulness of data personal. If implemented, indicate the form that was used. If it has not been implemented, indicate the reason.	Developer Developer Developer Developer	SDLC-RGPD-PR03-Doc.005V1.

Prepared by: <Developer Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

16. OBJETIVE AND SCOPE

Implementation of the right to updating of personal data by users, following the document of the design phase SDLC-RGPD-PR02-Doc005v1

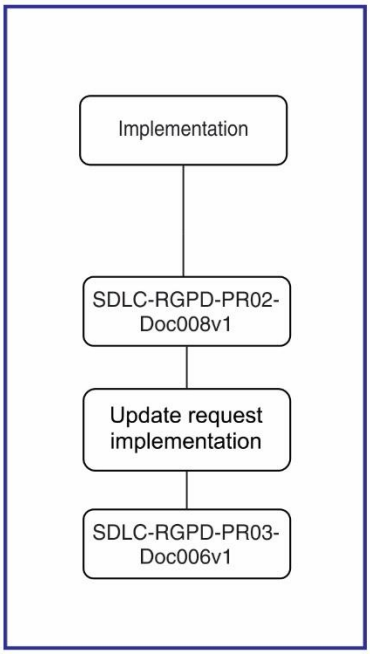
17. ABREVIATURAS E TERMOS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

18. MODE OF PROCEDURE

18.1 Implementation Document:: Doc006v1

18.1.1 Documento Controlo SDLC - RGPD

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Follow the phase document drawing RIGHTS OF PII HOLDERS - UPDATE. Fill document Order implementation data update personal. If implemented, indicate the form that was used. If it has not been implemented, indicate the reason.	Developer Developer Developer Developer	SDLC-RGPD-PR03-Doc.006V1.

Prepared by: <Developer Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

19. OBJETIVE AND SCOPE

Implementation of other orders
regarding personal data
by users,
following the document
of the drawing phase
SDLC-RGPD-PR02-Doc009v1

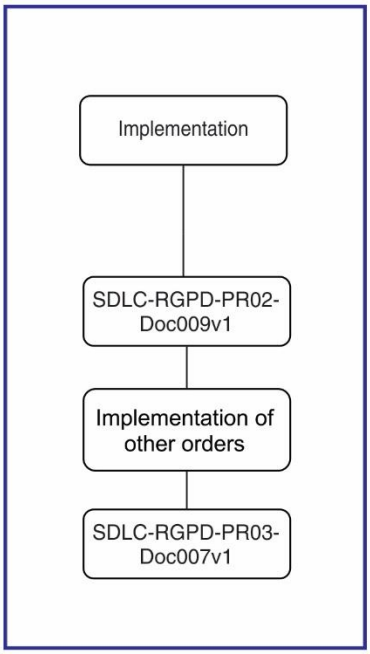
20. ABREVIATURAS E TERMOS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

21. MODE OF PROCEDURE

21.1 Implementation Document: Doc007v1

21.1.1 Documento Controlo SDLC - RGPD

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Follow the phase document drawing RIGHTS OF PII HOLDERS - <SPECIFY>. Fill document Implementation of other orders regarding personal data. If implemented, indicate the form that was used. If it has not been implemented, indicate the reason.	Desenvolvedor Desenvolvedor Desenvolvedor Desenvolvedor	SDLC-RGPD-PR03-Doc.007V1.

Prepared by: <Developer Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

CONSENT, PRIVACY AND TERMS & CONDITIONS

Has the PII collection and treatment consent been implemented? Yes ☐ No ☐ Not applicable ☐

If YES indicate:

What shape was it implemented?	Web pag and link	☐	Observations: indicate here the link, email template or form used in the implementation of the consent for the collection and treatment of personal data. If you have made changes to the consent model received in previous phases, please indicate here what changes you have made.
	Form	☐	
	Email	☐	
	Other	☐	
How is consent being kept?			
Not being saved	☐		
It is being saved	☐ (indicate below how)		
Comments:			

If requested and NOT implemented, tell us why:

Was the privacy policy model implemented in the application? Yes ☐ No ☐ Not applicable ☐

If YES indicate:

What shape was it implemented?	Web page and link	☐	Observations: indicate here the link, email template or form used in the implementation / disclosure of the privacy policy in force in the company. If you have made changes to the model received in previous phases, indicate here what changes were made.
	Form	☐	
	Email	☐	
	Other	☐	

How is the agreement (check) with the privacy policy being kept?	
Not being saved	☐
It is being saved	☐ (indicate below how)
Comments:	

If requested and NOT implemented, tell us why:

Was the terms and conditions model implemented in the application? Yes ☐ No ☐ Not applicable ☐

If YES indicate:

What shape was it implemented?	Web page and link	☐	Observations: indicate here the link, email template or form used in the implementation / disclosure of the terms and conditions for using the application. If you have made changes to the model received in previous phases, indicate here what changes you have made.
	Form	☐	
	Email	☐	
	Other	☐	
How is the agreement (check) being kept with the presented terms and conditions?			
Not being saved	☐		
It is being saved	☐ (indicate below how)		
Comments:			

If requested and NOT implemented, tell us why:

CONTROL OF ACCESS TO PERSONAL DATA ACCORDING TO ACCESS / DATA MATRIX (DATA MAPPING)

Access control was implemented according to the Access / Data Matrix? Yes ☐ No ☐ Partially ☐
Not applicable ☐

Is the database protected through encryption mechanisms? Yes ☐ No ☐

If you have fully or partially implemented access control, please indicate:

BD User / Profile and Field (s)	**Query/Vista implemented**	**Control adopted** (obfuscation, anonymization, ...)
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____

		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____
		Obfuscation☐ Anonymization☐ Other☐ _____

APPLICATION IMPLEMENTATION DATA ACCESS

Has the **right of access** to user data been implemented?

Yes ☐ No ☐ Not applicable ☐

If yes, please indicate:

How it was implemented?	Web page e link		Observations: indicate the form used in the implementation of the right of access to personal data by users. If you have made changes to the SDLC-RGPD-PR02-Doc005v1 document, please indicate here what changes you have made.
	Form		
	Email		
	Other		

If it was requested and NOT implemented, tell us why:

APPLICATION IMPLEMENTATION OF PORTABILITY

Has the **portability right** to user data been implemented?

Yes ☐ No ☐ Not applicable ☐

If YES indicate:

How was it implemented?	Web page and link		Observations: indicate the form used in the users' implementation of the right of portability to personal data. If you have made changes to the SDLC-RGPD-PR02-Doc006v1 document, indicate here what changes you have made.
	Form		
	Email		
	Other		

If it was requested and NOT implemented, tell us why:

APPLICATION IMPLEMENTATION FORGETTING

Has the right to forget user data been implemented?

Yes ☐ No ☐ Not applicable ☐

If YES indicate:

How was it implemented?	Web page and link		Observations: indicate the form used in the implementation of the right of users to forget personal data. If you have made changes to the SDLC-RGPD-PR02-Doc007v1 document, please indicate here what changes you have made.
	Form		
	Email		
	Other		

If if was requested and NOT implemented, tell us why:

APPLICATION IMPLEMENTATION UPDATE

Has the right to update user data been implemented?

Yes ☐ No ☐ Not applicable ☐

If YES indicate:

How was it implemented?	Web page and link		Observations: indicate the form used in the users' implementation of the right to update personal data. If you have made changes to the SDLC-RGPD-PR02-Doc008v1 document, indicate here what changes you have made.
	Form		
	Email		
	Other		

If it was requested and NOT implemented, tell us why:

IMPLEMENTATION OF
OTHER REQUESTS **<TO SPECIFY>**

Has another right to user data been implemented?

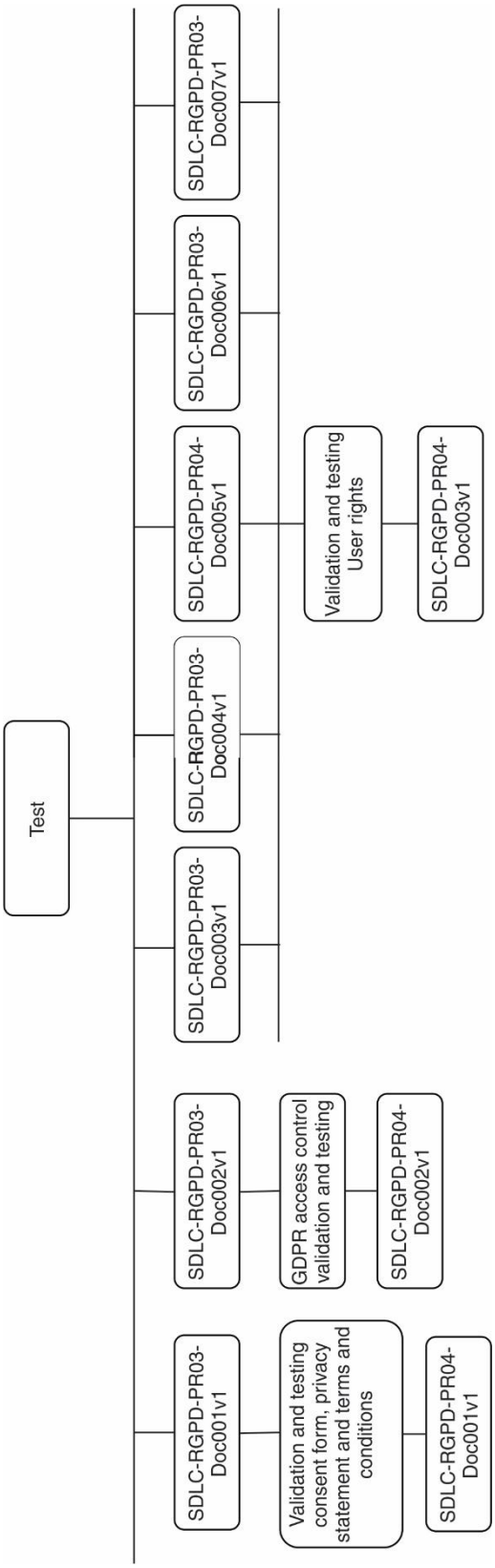
Yes ☐ No ☐ Not applicable ☐

Is YES indicate:

How was it implemented?	Web page and link		Observations: indicate the form used in the implementation of the other <SPECIFICAR> right to personal data by users. Indicate changes to the SDLC-RGPD-PR02-Doc009v1 document.
	Form		
	Email		
	Other		

If it was requested and NOT implemented, tell us why:

Procedure 4 – Test



1. OBJETIVE AND SCOPE

Auditing the application and database data with a focus on PII.
Order validation and test consent, declaration of privacy and terms and conditions

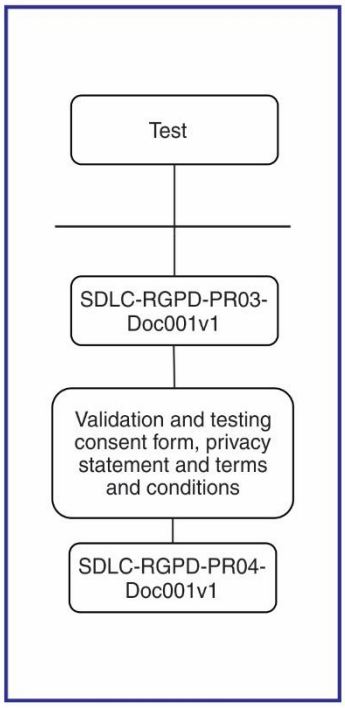
2. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

3. MODE OF PROCEDURE

3.1 Test Document: Doc001v1

3.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	During the SDLC Test phase, verify that implementation meets the GDPR through a security audit, with focus on protecting information personal data of the data subject. According to the document CONSENT, PRIVACY AND TERMS & CONDITIONS completed in the implementation phase: Perform the tests and complete the validation and test document consent request, declaration of privacy and terms and conditions	Test Team Test Team Test Team	SDLC-RGPD-PR04-Doc.001V1.

Prepared by: <Test Leader's Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

4. OBJETIVE AND SCOPE

Auditoria à aplicação e base de dados com enfoque na PII. Controlo de perfil e acesso, validação e teste de acordo com o RGPD.

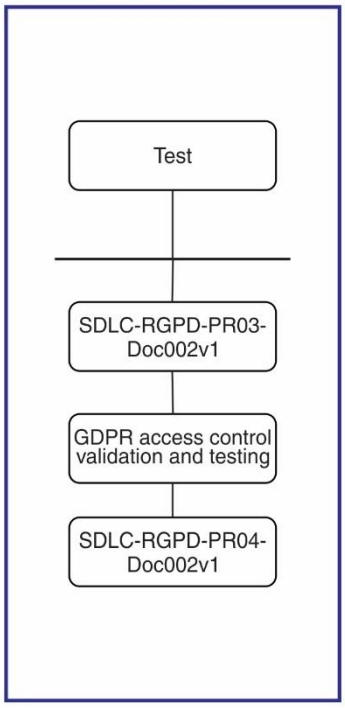
5. ABREVIATURAS E TERMOS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

6. MODE OF PROCEDURE

6.1 Test Document: Doc002v1

6.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	According to the document ACCESS CONTROL TO PERSONAL DATA AGREEMENT WITH ACCESS / DATA MATRIX (DATA MAPPING) completed in the implementation phase: Perform the tests and complete the validation and test document GDPR access control with the results.	Test Team Test Team	SDLC-RGPD-PR04-Doc.002V1.

Prepared by: <Test Leader's Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

7. OBJETIVE AND SCOPE

Auditing the application and database data with a focus on PII.
Validation and testing of rights of users on personal data (right of access, right of portability, right to forget, right to update or other implemented right)

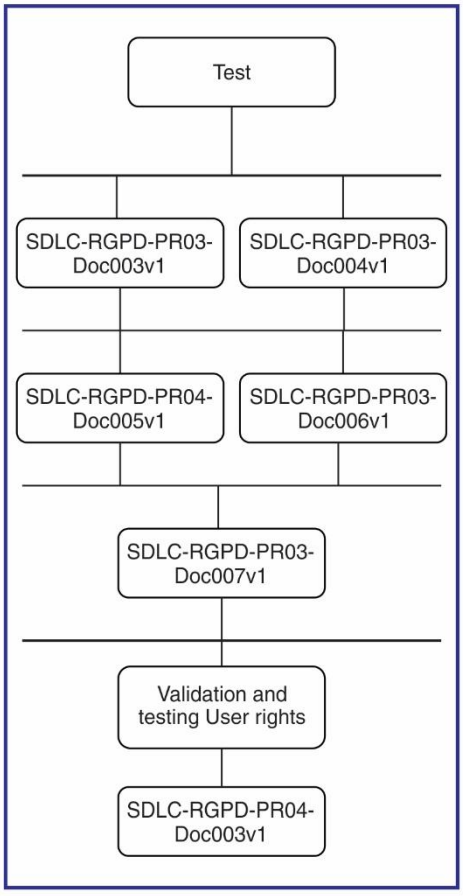
8. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1

9. MODE OF PROCEDURE

9.1 Test Document: Doc003v1

9.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	According to the documents APPLICATION IMPLEMENTATION OF ACCESS TO DATA, REQUEST FOR PORTABILITY, FORGETTING REQUEST, UPDATE, OTHER ORDERS, completed in the Implementation: Perform the tests and complete the Validation and Test document Rights of users with the results.	Test Team Test Team	SDLC-RGPD-PR04-Doc.003V1.

Prepared by: <Test Leader's Name>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

VALIDATION AND TESTING CONSENT REQUEST,
PRIVACY STATEMENT AND TERMS AND CONDITIONS

Request for consent from the data subject:

Implemented ☐ Tested ☐ According ☐ Not compliant ☐

Observations: <indicate reason for non-compliance>

Data privacy statement:

Implemented ☐ Tested ☐ According ☐ Not compliant ☐

Observations: <indicate reason for non-compliance>

Terms and conditions:

Implemented ☐ Tested ☐ According ☐ Not compliant ☐

Observations: <indicate reason for non-compliance>

Test result:

VALIDATION AND TEST GDPR ACCESS CONTROL

Profile/ User	**Form/Option**	**Control adopted** (obfuscation, anonymization, …)	**Validation/Testing**	**Observations**
		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	
		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	
		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	
		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	

		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	
		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	
		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	
		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	
		Obfuscation ☐ Anonymization ☐ Other ☐ ______________	Implemented ☐ Tested ☐ According ☐ Not Conforming ☐	

VALIDATION AND TESTING RITHTS FROM USERS

Request for **access** to personal data:
Implemented ☐ Tested ☐ According ☐ Not conform ☐

Observations:

Request for **portability** of personal data:
Implemented ☐ Tested ☐ According ☐ Not conform ☐

Observations:

Request for **forgetting** personal data by the data subject:
Implemented ☐ Tested ☐ According ☐ Not conform ☐

Observations:

Request for **updating** of personal data by the data subject:
Implemented ☐ Tested ☐ According ☐ Not conform ☐

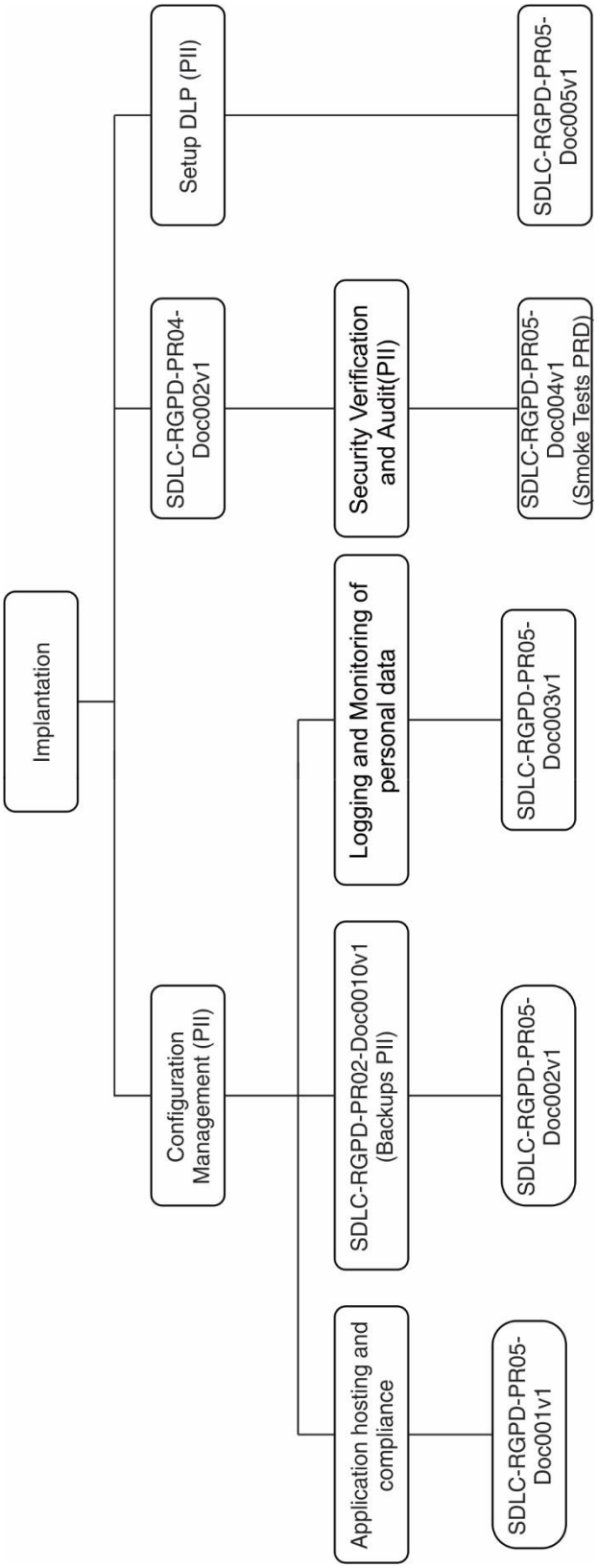
Observations:

Another type of request for personal data by the data subject:
Implemented ☐ Tested ☐ According ☐ Not conform ☐

Observations:

Test result:

Procedure 5 - Implantation



Specification Documents Deployment:

1. OBJETIVE AND SCOPE

Make the application available on production environment with risk protection mechanisms and PII protection. Perform the Management of Settings (PII) and check Hosting application and GDPR compliance.

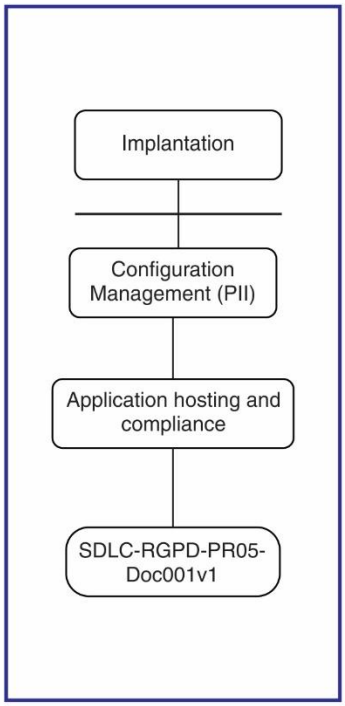
2. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1
DLP - Data loss prevention

3. MODE OF PROCEDURE

3.1 Implantation Document: Doc001v1

3.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	In the SDLC Implementation phase, after pass the test audit in GDPR compliance, carry out Configuration Management (PII). Fill in the document ACCOMMODATION APPLICATION AND COMPLIANCE, according to Accommodation Application (binary) and check the type of accommodation, type of accommodation, the Management and whether they are in compliance or not with the GDPR. Also fill in the Accommodation table Application data (Storage) and check the if the storage is internal or external, type Storage, Management console and presence or not of conformity with the GDPR.	Production Team Production Team Production Team	SDLC-RGPD-PR05-Doc.001V1.

Prepared by: <Name of Responsible for the Deployment>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

4. OBJETIVE AND SCOPE

Still in Configuration Management (PII), following the phase backup document validated design, check that the PII backups are in compliance with the GDPR ensuring security personal data.

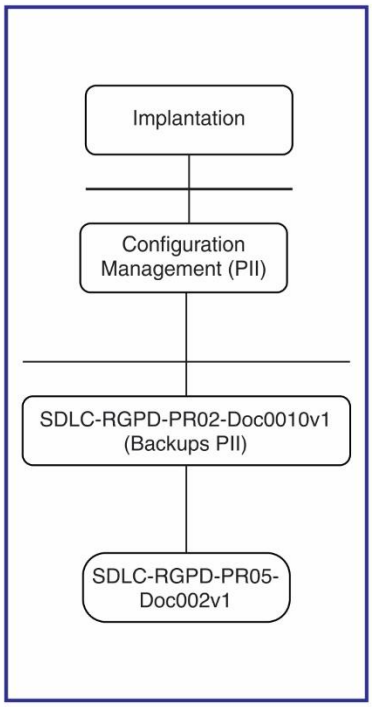
5. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1
DLP - Data loss prevention

6. MODE OF PROCEDURE

6.1 Implantation Document: Doc002v1

6.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Continue Configuration Management (PII) of the deployment phase to verify comply with backups of according to the GDPR. Following the validated document in the drawing phase regarding Backups of the PII, also complete the document PERSONAL DATA BACKUPS in phase application deployment. Verify that backups are internal or external, Backup type. Besides that, indicate whether backups and restores have been tested and whether they have been according to the plan.	Production Team Production Team Production Team	SDLC-RGPD-PR05-Doc.002V1.

Prepared by: <Name of Responsible for the Deployment>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

7. OBJETIVE AND SCOPE

Também dentre os documentos da Gestão de Configurações (PII), encontra-se o documento para fazer a verificação do Logging e monitorização de dados pessoais, garantindo o registro de acesso às PII.

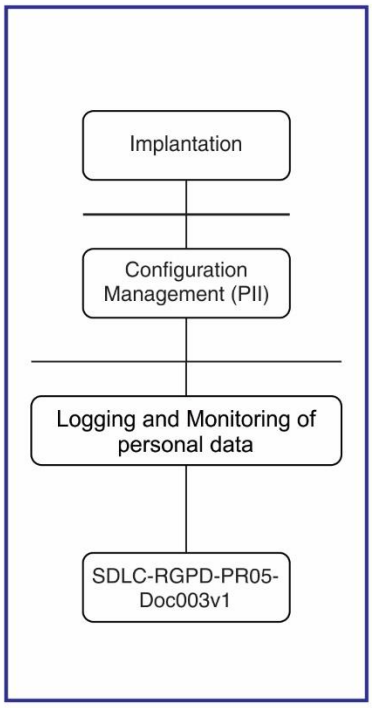
8. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1
DLP - Data loss prevention

9. MODE OF PROCEDURE

9.1 Implantation Document: Doc003v1

9.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Still in Configuration Management (PII) implementation phase, check the Logs and Data Monitoring personal data are in accordance with regulation. Complete the LOGGING E document MONITORING PERSONAL DATA. Check registered access control log, log monitoring and access data, access (read, change, remove) and the rights exercised by logged users.	Production Team Production Team Production Team	SDLC-RGPD-PR05-Doc.003V1.

Prepared by: <Name of Responsible for the Deployment>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

10. OBJETIVE AND SCOPE

Após ser validado o teste controlo de acessos RGPD no documento da fase anterior, realizar a verificação e auditoria de segurança (PII) baseado no Smoke Test PRD, informando os tipos de filtro, log de acesso, log de direto, soluções DLP e backups, de segurança de acordo com o RGPD.

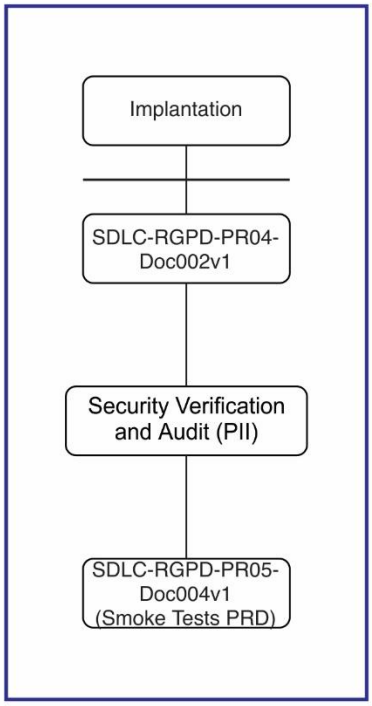
11. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1
DLP - Data loss prevention

12. MODE OF PROCEDURE

12.1 Implantation Document: Doc004v1

12.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check the completed document in the test phase, Validation and test control of GDPR accesses. Fill in the document VERIFICATION AND SECURITY AUDIT (PII) (SMOKE TESTS PRD). Check if the data is filtered according to according to the application profile. If so, inform the type of filter applied. Inform the type of log application access, rights log, how replacement of an backup, security of backups of personal data and the DLP solution.	Production Team Production Team Production Team	SDLC-RGPD-PR05-Doc.004V1.

Prepared by: <Name of Responsible for the Deployment>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

13. OBJETIVE AND SCOPE

Realizar o preenchimento
do documento de setup DLP (PII)
e verificar se existe algo na aplicação
que afeta o DLP e os tipos de controlos
ativados para a aplicação ficar em
conformidade com o RGPD, validando
a implantação do sistema.

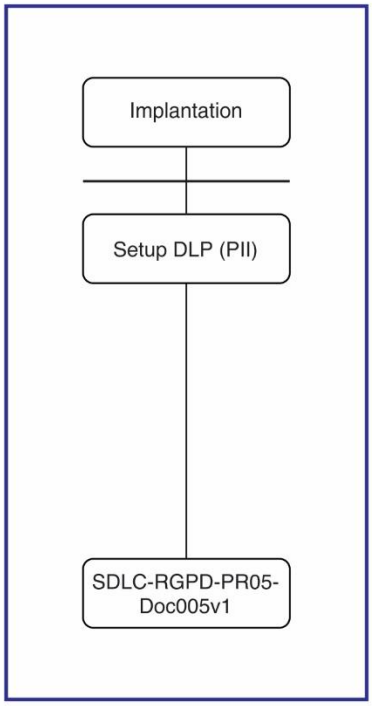
14. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
CC - Citizen Card
Doc - Document
v1 - Version 1
DLP - Data loss prevention

15. MODE OF PROCEDURE

15.1 Implantation Document: Doc005v1

15.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Complete the SOLUTION document DATA LOSS PREVENTION, check that is there any solution in the application that affects DLP. If so, identify the controls and whether or not they are activated in the system. Also identify the types of monitoring covered by the solution DLP and examples of controls activated.	Production Team Production Team	SDLC-RGPD-PR05-Doc.005V1.

Prepared by: <Name of Responsible for the Deployment>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

APPLICATION ACCOMMODATION (Binaries)

Accommodation	Accommodation type	Management Console	GDPR compliance
Internal ☐	Dedicated server ☐ Shared Server ☐ Private Cloud ☐ Other ☐ _____	Internal Personal Access ☐ External Personal Access ☐ Other ☐ _____	Yes ☐ No ☐ N.A. ☐
External ☐	Dedicated server ☐ Shared Server ☐ Private Cloud ☐ Cloud Pública ☐ Other ☐ _____	Internal Personal Access ☐ External Personal Access ☐ Other ☐ _____	Yes ☐ No ☐ N.A. ☐
Obs:			

DATA ACCOMMODATION APPLICATION (Storage)

Storage	Type storage	Management Console	GDPR compliance
Internal ☐	Dedicated ☐ Shared ☐ In conjunction with the application ☐ Encrypted ☐ Other ☐ _____	Internal Staff ☐ External Staff ☐ Other ☐ _____	Yes ☐ No ☐ N.A. ☐
External ☐	Dedicated ☐ Shared ☐ In conjunction with the application ☐ Encrypted ☐ Other ☐ _____	Internal Staff ☐ External Staff ☐ Other ☐ _____	Yes ☐ No ☐ N.A. ☐
Obs:			

BACKUPS PERSONAL DATA

Backups	Type of backups	Tested Backup and Restore	Implemented according to plan
Internal ☐	Online ☐ Offline ☐ Other ☐ _____	Yes ☐ No ☐	Yes ☐ No ☐
External ☐	Online ☐ Offline ☐ Other ☐ _____	Yes ☐ No ☐	Yes ☐ No ☐
Obs:			

LOGGING AND MONITORING OF PERSONAL DATA

Logged access control: Yes ☐ No ☐

Log and format (example):

There is monitoring on the access control log: Yes ☐ No ☐

Alert and destination:

Access (read, change, remove) to personal data logged: Yes ☐ No ☐

Log and format (example):

Is there monitoring on access to personal data: Yes ☐ No ☐

Alert and destination:

Rights exercised by users kept on log: Yes ☐ No ☐

Access	**Log and format (example):**
Forgetfulness	**Log and format (example):**
Update	**Log and format (example):**
Portability	**Log and format (example):**
Other: _____ _____	**Log and format (example):**

Is there monitoring on rights exercised by users of personal data: Yes ☐ No ☐

Alert and destination:

Security verification and auditing (PII)
(Smoke testS PRD)

Is the data filtered according to the application profile? Yes ☐ No ☐

If yes, indicate the types of filters applied:

Filters	Applied / Not Applied	Observation
Obfuscation	Yes ☐ No ☐	
Anonimization	Yes ☐ No ☐	
Other: _____	Yes ☐ No ☐	

Is the application access log logged? Yes ☐ No ☐

Log Type

Is the rights exercised on users logged? Yes ☐ No ☐

Rights log (example):

When replacing a backup, is it guaranteed that user data that is out of date, non-existent at the date is not restored? Yes ☐ No ☐

How a backup is performed:

Before the attack (example: ransomware) are backups not affected? Yes ☐ No ☐

Security of personal data backups:

Is there a DLP solution that monitors and controls access to personal data? Yes ☐ No ☐

DLP solution (example):

DATA LOSS PREVENTION SOLUTION

Is there any DLP solution affecting the application: Yes ☐ No ☐

If yes, indicate which of the controls have been activated for the application:

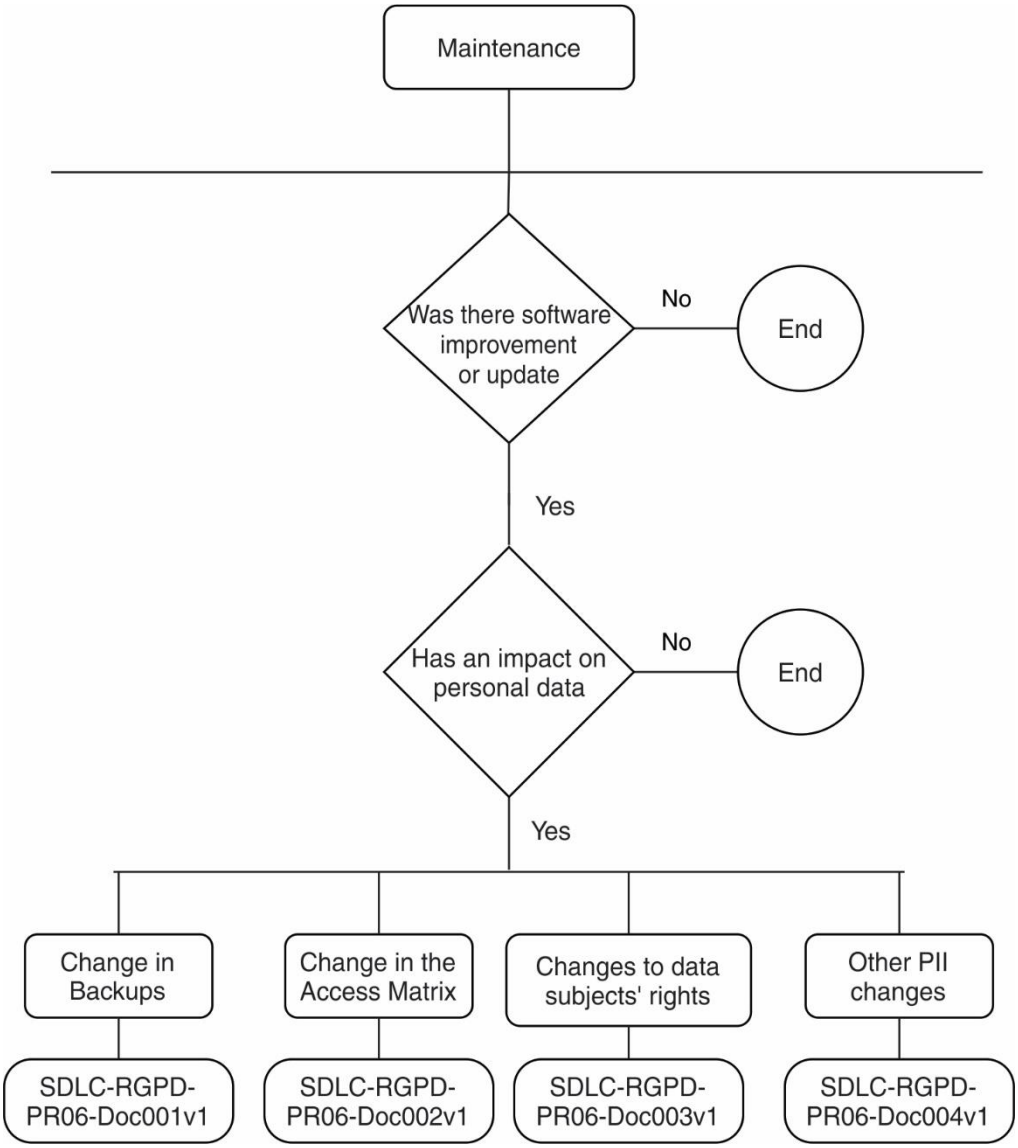
Control	Activated?
Identification of personal / sensitive data	Yes ☐ No ☐
Classification of personal / sensitive data	Yes ☐ No ☐
Monitoring of activities involving personal / sensitive data	Yes ☐ No ☐

Indicate the types of monitoring covered by the DLP solution:

Monitoring type	Controls enabled
Data at rest	Restrict access to local administrative functions, such as the ability to install software and modify security settings. Prevent malware, viruses, spyware, etc. Prevent copying of confidential data on unapproved media. Verify that authorized data extraction occurs only on encrypted media.
Data in use	Monitor access and use of high-risk data to identify potentially inappropriate use. Restrict user skills to copy sensitive data into unapproved containers (for example, email, web browsers), including control over the ability to copy, paste and print sections of documents.
Data in motion	Prevent unencrypted sensitive data from leaving the perimeter. Record and monitor network traffic to identify and investigate inappropriate transfers of sensitive data.

Active monitoring of Data Leaks	Verify that remote access to the corporate network is protected and control data that can be saved through remote installations, such as Outlook Web Access.

Procedure 6 - Maintenance



Specification Documents Manutenção:

MAINTENANCE **SDLC-RGPD-PR06-Doc001v1**
SDLC PHASE - MAINTENANCE

1. OBJETIVE AND SCOPE

Regular application security testing and PII and after updates, management application versions and GDPR audits.
Backup copies.
Check for changes in the backups that affect the save personal information.

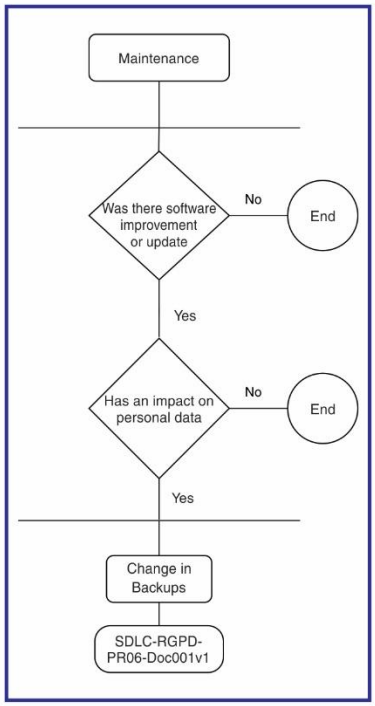
2. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
Doc - Document
v1 - Version 1

3. MODE OF PROCEDURE

3.1 Maintenance Document: Doc001v1

3.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Check for improvement or software update. If there was no change in the software is the end of the process. If there was an improvement or update, check if it has an impact on the data personal. If the changes had no impact in personal data is the End. If there was an impact on personal data: Document number Change in Backups record the date and the person responsible for change and updates made.	Maintenance team Maintenance team Maintenance team	SDLC-RGPD-PR06-Doc.001V1.

Prepared by: <Name of Responsible for the for maintenance>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

4. OBJETIVE AND SCOPE

Regular application security testing
and PII and after updates, management
application versions and GDPR audits.
Check for changes
in the access matrix that affect
personal data.

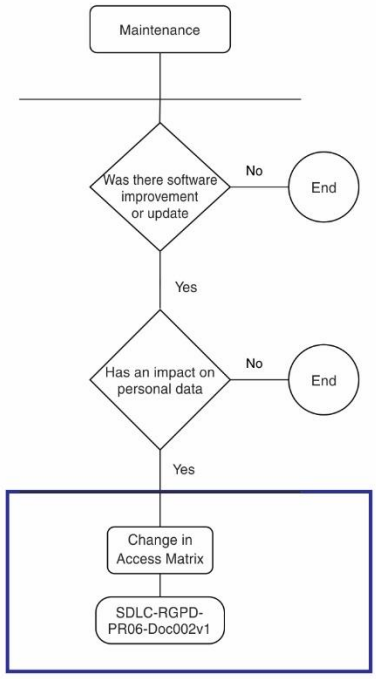
5. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
Doc - Document
v1 - Version 1

6. MODE OF PROCEDURE

6.1 Maintenance Document: Doc002v1

6.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	In the document Change in the Matrix Access, register only the changes affecting personal data, with the date that is held and the responsible for the change.	Maintenance team	SDLC-RGPD-PR06-Doc.002V1.

Prepared by: <Name of Responsible for the for maintenance>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

7. OBJETIVE AND SCOPE

Also among the documents Configuration Management (PII), is the document for check the Logging and monitoring of personal data, ensuring access record at PII.

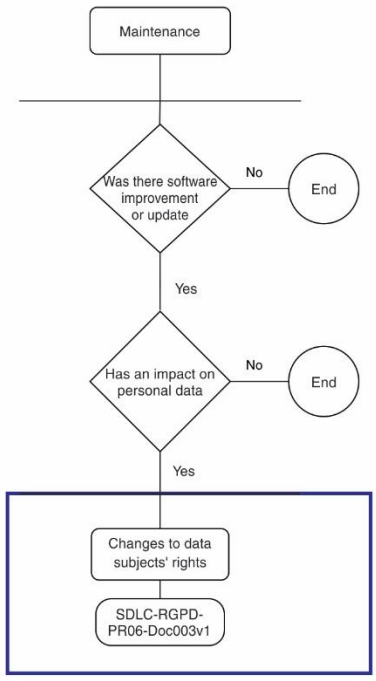
8. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
Doc - Document
v1 - Version 1

9. MODE OF PROCEDURE

9.1 Maintenance Document: Doc003v1

9.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Register in the document Amendment Right of Users the changes that affect and impact personal data application.	Maintenance team	SDLC-RGPD-PR06-Doc.003V1.

Prepared by: <Name of Responsible for the for maintenance>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

10. OBJETIVE AND SCOPE

After the control test has been validated of GDPR accesses in the document previous phase, perform the verification and security audit (PII) based on Smoke Test PRD, informing the types of filter, access log, direct log, DLP solutions and backups, security in accordance with the GDPR.

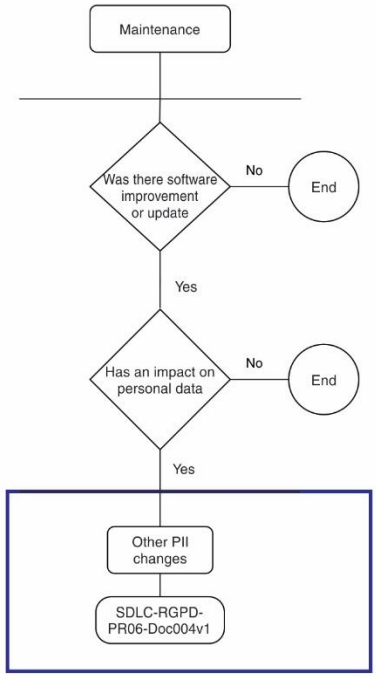
11. ABBREVIATIONS AND TERMS

GDPR - General Data Protection Regulation
SDLC - Software Development Cycle
DPO - Responsible for data processing
PII - Personally Identifiable Information
Doc - Document
v1 - Version 1

12. MODE OF PROCEDURE

12.1 Maintenance Document: Doc004v1

12.1.1 SDLC Control Document - GDPR

ACTIVITIES	DESCRIPTION	RESP.	DOC.
	Register in the document Other Changes PII and specify which change was made and the content that will affect the data personal data in the software.	Maintenance team	SDLC-RGPD-PR06-Doc.004V1.

Prepared by: <Name of Responsible for the for maintenance>	Verified by: <DPO name>	Approved by: <Name of the Project Manager>
Date: <Year-month-day>	Date: <Year-month-day>	Date: <Year-month-day>

CHANGE IN PERSONAL DATA BACKUPS - DATA AT REST

1 – Change in the information collected from the requirements specification and analysis phase

Have there been changes to backups that affect the safeguarding of personal data: Yes ☐ No ☐

If YES, describe changes to the backup plan:

Type	Frequency	Type	Safety	Local
Total	Daily ☐ Weekly ☐ Monthly ☐ Other _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Incremental	Daily ☐ Weekly ☐ Monthly ☐ Other _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Archive logs	Size _____	Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐
Other		Offline ☐ Online ☐	Encrypted ☐ Unencrypted ☐	Onsite ☐ Offsite ☐

Observations regarding changes:

Date: ___ / ___ /_____ Name: _____

ALTERAÇÃO NA MATRIZ DE ACESSOS / DADOS (DATA MAPPING)

Houve alterações nos backups que afetam a salvaguarda de dados pessoais: Sim ( ) Não ( )

Se SIM descreva alteração do plano de backups:

Data da alteração: ___/ ___/____ **Nome:**

INSTRUÇÕES: **SÓ DEVEM SER REGISTADAS AS ALTERAÇÕES!**
Especificar os campos da BD relativos às **alterações** dos dados pessoais/sensíveis na linha 6
Especificar **alterações** dos utilizadores/perfis na coluna A

Completar com S/N sendo "S" da **alteração** na indicação de operação permitida sobre os campos pelo utilizador/perfil e "N" a indicação de acesso proibido/desnecessário do utilizador/perfil correspondente

Função / Campo e Operações	Primeiro Nome				Sobrenome				Último nome				Telefone				Morada				Email				NIF				NISS				Género				Empresa				Tu
	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C	R	U	D	C
admin		S		S				S				S		S		S				S		S		S				S				S		S		S		S		S	
rh				S				S				S				S				S				S				S				S		S		S		N		N	
inf				S				N				N				N				N				N				N				N		S		S		N		N	
ana@xpto.com				N				N				N				N				N				N				N				N		S		S		S		S	
manuel@xpto.com				S				N				N				S				N				S				N				N		S		S		S		S	
DPO				S				S				S				S				N				S				S				S		S		S		S		S	

...				S				S				S				S				S				S				N				N		S		S		S		S		S		S		N		N		N		N		N		N

CHANGING USER RIGHTS

Right	Changed	Format	Observations of Changes
Access	Yes ☐ No ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in legal warning ☐ Other ☐	
Portability	Yes ☐ No ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in legal warning ☐ Other ☐	
Forgetfulness	Yes ☐ No ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in legal warning ☐ Other ☐	
Update	Yes ☐ No ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in legal warning ☐ Other ☐	
	Yes ☐ No ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in legal warning ☐ Other ☐	
	Yes ☐ No ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in legal warning ☐ Other ☐	
	Yes ☐ No ☐	Email ☐ Portal ☐ Application form ☐ Warning ☐ Included in legal warning ☐ Other ☐	

Date: ___ / ___ /_____ Name: _____

Other PII changes <To specify >

Was there software improvement or update: Yes ☐ No ☐

Does it have an impact on personal data: Yes ☐ No ☐

If both YES indicate:

Change <To specify>	
Content	
Observations	

Se NO indicate:

What affects changes to the software?	
Specify changes	

Date: ___ / ___ /_____ Name: _____