UNIVERSIDADE CATÓLICA PORTUGUESA

Implementação do Regulamento Geral sobre a Proteção de Dados em Gestão de Pessoas

O caso da Nors, S.A.

por

Rui Miguel Barros Rouxinol

Católica Porto Business School
Abril, 2024

UNIVERSIDADE CATÓLICA PORTUGUESA

Implementação do Regulamento Geral sobre a Proteção de Dados em Gestão de Pessoas

O caso da Nors, S.A.

Trabalho Final na modalidade de Relatório de Estágio
apresentado à Universidade Católica Portuguesa
para obtenção do grau de mestre em Gestão

por

Rui Miguel Barros Rouxinol

sob orientação de
Prof. Doutora Ana Lourenço

Católica Porto Business School
Abril, 2024

Agradecimentos

Este trabalho não teria sido possível sem o suporte de algumas pessoas, que de alguma forma contribuíram para este grande desafio.

Em primeiro lugar, à minha família por me ter proporcionado a oportunidade de integrar um curso de gestão numa universidade tão consagrada como a Católica Porto Business School.

À minha orientadora, Professora Ana Lourenço, por toda a disponibilidade, e apoio sempre demonstrado ao longo da realização deste trabalho.

Importa também agradecer ao Grupo Nors, mais concretamente a todos os entrevistados da Nors pela ajuda e disponibilidade que demonstraram em todo o processo de investigação.

Por fim, à minha namorada e a todos os meus amigos, pela força e resiliência que me transmitiram nesta jornada.

Resumo

A proteção de dados assume uma importância cada vez mais crucial na sociedade contemporânea, marcada pela proliferação de tecnologias digitais e pela crescente dependência de informação. No âmbito empresarial, esta proteção assume uma relevância ainda mais significativa, sendo que a sua implementação contribui para reforçar a confiança dos clientes e parceiros; mitigar riscos e sanções; e aumentar a eficiência e produtividade.

O presente trabalho tem como objetivo perceber, na área de gestão de pessoas, quais são as fases da implementação do Regulamento Geral sobre a Proteção de Dados (RGPD), quais são os desafios enfrentados nessa implementação, quais são as vantagens e, por fim, quais são as oportunidades de melhoria nos processos de proteção de dados. O interesse neste tema surgiu no contexto de um estágio realizado na área de gestão de pessoas da Nors, S.A.

De forma a responder a este conjunto de questões de investigação, foi realizado um estudo de caso sobre a implementação do RGPD no Grupo Nors. O estudo teve por base entrevistas semiestruturadas e documentos cedidos pela organização.

A análise dos dados recolhidos permitiu concluir que a implementação do RGPD no Grupo Nors,, organizada através de um processo planeado em várias fases, trouxe aspetos positivos, mas também negativos, no quotidiano da empresa. No que concerne aos benefícios, a implementação trouxe uma maior proteção aos dados pessoais dos colaboradores; impulsionou a mudança em certos processos antiquados e diminuiu o risco inerente à falta de proteção de dados. Por outro lado, o decorrer do levantamento dos dados e processos associados ao RGPD foi caracterizado pela grande dimensão da base de dados de clientes, repleta de informações pessoais, que dificultou e atrasou este

processo. Adicionalmente foi percecionado que não existe nenhum programa que fosse capaz de lidar com as exigências deste regulamento. Para além disso, concluiu-se que existem algumas lacunas nos procedimentos que visam salvaguardar os dados pessoais, que há que solucionar, nomeadamente aquando da realização da admissão do colaborador, já que todos os dados pessoais requeridos para a realização do contrato de trabalho revertem para formato de papel e o seu nível de segurança diminui, uma vez que ficam ao dispor de de "qualquer um".

Palavras-chave: RGPD; Gestão de Pessoas; Proteção de Dados; Digitalização

Abstract

Data protection assumes an increasingly crucial importance in contemporary society, marked by the regulation of digital technologies and growing dependence on information. In the business sphere, this protection assumes even more significant relevance, with its implementation helping to reinforce the trust of customers and partners; mitigate risks and assessments; and increase efficiency and productivity.

The present work aims to understand, in the area of people management, what are the phases of implementing the General Data Protection Regulation (GDPR), what are the challenges faced in this implementation, what are the advantages and, finally, what are the opportunities for improvement in data protection processes. The interest in this topic arose in the context of an internship carried out in the people management area of Nors, S.A.

To answer this set of research questions, a case study was carried out on the implementation of the GDPR in the Nors Group. The study was based on semi-structured interviews and documents provided by the organization.

The analysis of the data collected allowed us to conclude that the implementation of the GDPR, organized through a planned process in several phases, brought positive, but also negative, aspects to the company's daily life. With regard to benefits, the implementation brought greater protection to employees' personal data; it drove change in certain antiquated processes and reduced the risk caused by a lack of data protection. On the other hand, the collection of data and processes associated with the GDPR was characterized by a gigantic customer database full of personal information that made this process difficult and delayed. Additionally, it was noticed that there is no program that is capable of dealing with the criteria of this regulation.Furthermore, we

concluded that there are some gaps in the procedures aimed at the security of personal data, which must be resolved, namely, when the employee is hired, all personal data necessary for the execution of the employment contract reverts to paper format and their level of security decreases since they are at the mercy of "anyone".

Keywords: GDPR; People management; Data Protection; Digitization

Índice

Índice de Figuras

Índice de Tabelas

Índice de Gráficos

Abreviaturas e Acrónimos

CNPD- Comissão Nacional de Proteção de Dados

DGP- Departamento de Gestão de Pessoas

DJ- Departamento Jurídico

DPO- Encarregado de Tratamento de Dados Pessoais

DRH- Departamento de Recursos Humanos

RGPD- Regulamento Geral sobre a Proteção de Dados

Introdução

O presente Trabalho Final de Mestrado (TFM) corresponde à modalidade Relatório de Estágio tendo este sido realizado no Departamento de Gestão de Pessoas, no Grupo Nors, com a duração de cerca de 5 meses: iniciou a 15 de setembro de 2023 e terminou a 29 de fevereiro de 2024.

No decurso do estágio, em especial no âmbito do processo de admissão de colaboradores, o tema da proteção de dados pessoais à luz do Regulamento Geral sobre Proteção de Dados Pessoais (RGPD) tornou-se saliente, pelo que este trabalho procurou explorar as seguintes questões de investigação:

Q1: "Quais são as fases de implementação do RGPD?"

Q2: "Quais são os principais desafios e dificuldades na sua implementação?"

Q3: "Quais são as principais vantagens?"

Q4: "Quais são as oportunidades de melhoria nos processos de proteção de dados?"

Estas questões são exploradas a partir do estudo de caso da implementação do RGPD no Grupo Nors, das principais dificuldades na sua implementação, das vantagens obtidas e por último, dos pontos em que o processo de proteção de dados no Departamento de Gestão de Pessoas (DGP) pode ser melhorado.

Estas questões surgiram pelo crescimento, na última década, da hiperconectividade experienciada diariamente. Esta recente característica

mundial é marcada por um fluxo constante de dados, impulsionado pela internet e tecnologias móveis, sendo que esta transferência de dados, que se dá em tempo real, molda a maneira como comunicamos, trabalhamos, nos relacionamos, consumimos e viajamos (Poosarla, 2022).

Já no âmbito empresarial, esta hiperconectividade traduz-se numa série de vantagens, tais como o aumento de eficiência na comunicação interna, com o recurso a diversas ferramentas tecnológicas como email, mensagens instantâneas e videoconferência, que acabam por facilitar o contacto entre equipas e departamentos. De facto, segundo Holá & Pikhart (2014) a comunicação interna tem um papel fundamental no sucesso de uma empresa, pois garante que os colaboradores estejam informados e alinhados com a estratégia da mesma e permite também uma maior eficácia na concretização de trabalhos, tudo isto apoiado pelas novas tecnologias. No entanto, essa conectividade constante também traz consigo alguns riscos, sendo os mais relevantes os que se prendem com a questão da segurança dos dados, que atualmente obriga as empresas a investir em medidas para proteger informações confidenciais contra ataques informáticos. Como é possível verificar através da figura 1, o volume de mercado de softwares e serviços de dados, incluindo a proteção dos mesmos, vai aumentar significativamente nos próximos 20 anos.

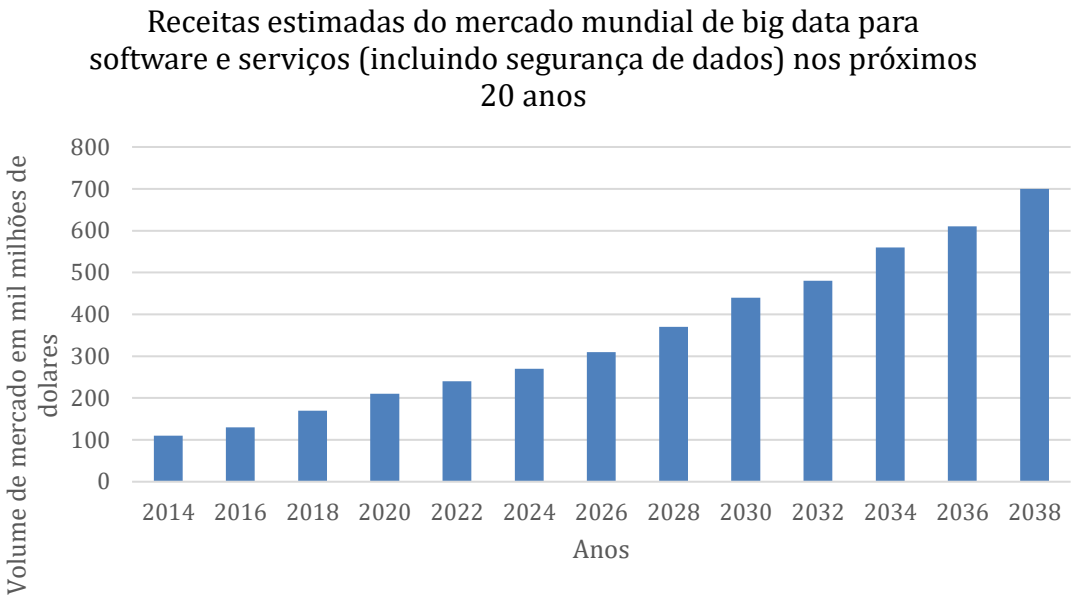


Gráfico 1. Receitas estimadas do mercado mundial de big data para software e serviços (incluindo segurança de dados) nos próximos 20 anos. Fonte: Tao et al. (2019)

Tao et al. (2019) defendem que à medida que o fluxo de informação em formato digital aumenta, a probabilidade de ciberataques aumenta também, e de forma exponencial, sendo que um vasto volume de dados consolidados pode tornar-se facilmente atrativo para os ciber criminosos, especialmente se estes dados forem de caráter sigiloso.

Por outro lado, o excesso de informação não útil torna-se prejudicial, comprometendo a produtividade. Para Borkovich (2017) os colaboradores têm dificuldades em gerir o excesso de informação num ambiente organizacional, fruto das fronteiras entre as responsabilidades profissionais e pessoais se tornarem ténues pelo uso de dispositivos tecnológicos obrigatórios pela empresa, exigindo quase uma disponibilidade de "24/7/365."

O método escolhido para melhor responder às questões de investigação é o caso de estudo de uma organização, neste caso do Grupo Nors, encabeçado pela Nors, S.A. Este método permite, através da análise e do estudo de uma situação real e contemporânea, obter mais informações e dados relevantes sobre um determinado tema (Aberdeen, 2013). A recolha de dados para a construção do

caso foi feita através de entrevistas semiestruturadas a diversos colaboradores, de forma a recolher informação o mais fidedigna possível. Para além disso, foram também analisados diversos documentos cedidos pela empresa, relativos ao RGPD e à sua implementação.

A estrutura deste Trabalho Final de Mestrado é composta por cinco capítulos. No primeiro, realiza-se a revisão de literatura sobre a proteção de dados e o respetivo regulamento, o seu contexto histórico, a importância da sua aplicação e alguns conceitos chave; aborda-se também a importância da proteção de dados na área de gestão de pessoas numa organização e o seu grau de envolvência com dados pessoais;. por fim, apresenta-se a vertente de otimização de processos,. O segundo capítulo trata do método seguido neste trabalho, incluindo os respetivos objetivos, questões de investigação e técnicas de recolha e análise de dados. O terceiro capítulo caracteriza o Grupo Nors S.A., a fim de facultar o contexto do estudo, abordando a história da organização, os resultados financeiros nos últimos cinco anos e focando em particular o Departamento de Gestão de Pessoas (DGP). O quarto capítulo apresenta e discute os resultados do estudo. Por último, o quinto capítulo conclui o trabalho, dando resposta às questões de investigação e propondo pistas para futuros trabalhos.

Capítulo 1

1. A proteção de dados e a gestão de pessoas

1.1 Contexto histórico da proteção de dados

Atualmente, vivemos numa sociedade caracterizada pela hiperconectividade. Este fenómeno surge da constante ligação entre indivíduos, facilitada pela evolução da tecnologia, que permite às pessoas estarem em constante comunicação e consequentemente a serem bombardeados com nova informação (Poosarla, 2022).

De facto, no setor empresarial, a evolução digital tem sido de enorme relevância e de grande crescimento. As empresas estão cada vez mais a converter grande parte dos processos que anteriormente exigiam o formato papel para formato digital, com a ajuda de ferramentas tecnológicas (Parviainen et al., 2017). A título de exemplo temos a recolha, armazenamento e processamento de dados de forma mais rápida e organizada. Este processo traz benefícios significativos, como maior eficiência, produtividade e inovação, mas também apresenta riscos relacionados com a proteção desses mesmos dados.

Krivokapic (2018) afirma que estamos perante uma nova revolução industrial baseada em dados, poder de processamento e automatização, em que muitos Estados e entidades privadas têm a capacidade de recolher dados dos cidadãos de forma mais eficiente e conveniente do que alguma vez no passado. Tal inclui os movimentos efetuados nas redes sociais, hábitos alimentares e de lazer, pagamento pontual de dívidas e outras informações privadas. A recolha de dados é realizada de várias maneiras, como extrair dados de fontes publicamente disponíveis, utilizar técnicas especiais na internet, oferecer serviços aparentemente gratuitos em troca de dados comportamentais do utilizador, sem

consentimento direto, e, cada vez mais, adquirir dados junto de corretores de informações especializados (Schwab et al.,2011).

Em conformidade com a tendência geral de aumento do volume de informação que criamos, armazenamos ou disponibilizamos, a quantidade de informações sobre nós e as nossas características profissionais e pessoais aumentou significativamente nos últimos 10 anos (Schwab et al.,2011).

O aumento dos dados pessoais armazenados e disponíveis é possibilitado pelo desenvolvimento de tecnologias digitais e media, auxiliado pelo uso mais frequente de comunicações móveis, plataformas de redes sociais e ferramentas tecnológicas. Nesta corrida pelo acesso a dados, surgiu a questão acerca da propriedade dos mesmos: a quem é que pertencem os dados? Podem as pessoas livremente utilizar os seus próprios dados pessoais, como propriedade sua? E em que âmbito?

Na verdade, as tecnologias digitais inseridas na internet permitem inúmeras cópias de dados em diferentes processos, deixando assim os dados fora do controle dos indivíduos; consequentemente esta questão aponta definitivamente para a importância dos dados pessoais hoje e no futuro (Krivokapic et al., 2018).

1.2 A regulação de dados pessoais

Tendo em conta a evolução digital que se têm dado nos últimos anos, o RGPD emerge como uma resposta crucial, delineando normas e princípios na interseção entre os avanços tecnológicos e os direitos fundamentais consagrados na legislação. Este marco regulatório não só reflete a necessidade de adaptar a proteção de dados à era digital, como também incorpora os valores fundamentais consagrados no regulamento, estabelecendo assim uma base robusta para o

equilíbrio entre inovação tecnológica e respeito pelos direitos individuais (Christodoulou et al., 2020).

Thomsett (2017) descreve o Regulamento Geral sobre a Proteção de Dados (RGPD) como um novo regime de privacidade e proteção de dados da União Europeia, que entrou em vigor em 25 de maio de 2018. Este tem como objetivo principal fornecer uma maior proteção aos dados pessoais de indivíduos localizados na UE que, por consequência, impõe uma série de novas obrigações tanto às entidades de controlo como às que processam e armazenam esses mesmos dados. Adicionalmente, Jones & Kamiski (2020) afirmam que este regulamento é uma lei extensa e complexa, composta por 99 artigos e um prefácio com 173 secções, e que, devido a essa grande extensão e complexidade, acaba por existir, em certos temas, ambiguidade na sua aplicação. A título de exemplo, mesmo passados dois anos após a implementação do RGPD, indivíduos como advogados, juízes, professores e jornalistas continuam a interpretar a lei de forma errada, afirmando que o RGPD visa dar às pessoas o controlo total sobre as suas informações pessoais em todos os contextos (Patrick, 2019). Outros acreditam que o RGPD cria um direito de propriedade sobre os dados pessoais (Chakravort, 2020).

Na visão de Mikkelsen et al. (2017), as organizações tendem a lidar cada vez mais com uma grande quantidade de dados que, na grande maioria das vezes, incluem dados pessoais críticos e confidenciais sobre indivíduos, clientes ou funcionários. Este tipo de informação pode ser captado durante a atividade principal da empresa, como também através das redes sociais, media, sites ou até pelo feedback de empresas especializadas em estudar o comportamento do consumidor como forma de maximizar a proximidade ao cliente. Por esta razão, esses dados são considerados um recurso de valor incalculável, acarretando uma grande responsabilidade e riscos significativos que devem ser cuidadosamente salvaguardados, garantindo a sua confidencialidade e proteção contra roubo.

De facto, Chen et al. (2022) refere que o objetivo subjacente à adoção deste regulamento surgiu para consagrar aos indivíduos um maior controlo sobre os seus dados pessoais, ao mesmo tempo que encorajava as empresas a limitar a utilização desses dados para atividades como marketing. Aquando da especificação jurídica sob a qual uma empresa pode ou não processar dados pessoais, o RGPD tem efeitos de diversas maneiras. Por exemplo, desde a sua implementação, os websites estão impedidos de partilhar dados dos utilizadores com terceiros sem o seu consentimento, devendo este ser afirmativo, o que aumenta os custos da recolha de dados e diminui a capacidade das organizações de extrair dados pessoais.

Seguindo a mesma linha de raciocínio, o regulamento necessita de ter regras rigorosas sobre a forma como os dados pessoais dos clientes e dos colaboradores podem ser usados e protegidos, sendo que estas regras são aplicadas de forma direta e imparcial a todos os Estados Membros da União Europeia (UE), (Mikkelsen et al., 2017). Este regulamento proporciona aos residentes o direito de aceder, atualizar, corrigir, eliminar e transferir os seus dados pessoais. Isto significa que as empresas que pretendem tratar desses dados devem investir na criação ou compra de sistemas informáticos que cumpram estes direitos. Além disso, as empresas que exercem atividades com residentes na UE são obrigadas a encriptar e anonimizar quaisquer dados pessoais que armazenam. Devem também auditar os seus processos internos para garantir a conformidade, incluindo a nomeação de um responsável pela proteção de dados para supervisionar as atividades de gestão de dados. Consequentemente, os custos de conformidade (*compliance*) impostos às empresas são significativos, especialmente para aquelas cujo modelo de negócio assenta no tratamento de dados pessoais. De acordo com a PwC (2018), algumas empresas gastaram mais de 10 milhões de euros anualmente, no período entre maio de 2018 e o final de 2021, apenas na conformidade com o RGPD, desde que a lei se tornou aplicável.

Segundo Flanagan & Warren (2022) a potência do ecossistema de dados nunca foi tão grande, mas o sistema em si está a tornar-se mais difícil de navegar devido à crescente complexidade. Hoje em dia, partilhamos e recebemos dados diariamente para interagir com as tecnologias que nos servem, seja em contexto pessoal ou comercial. O ecossistema que processa os dados tem como função filtrar, usar e reutilizar esses mesmos dados, geralmente para fins comerciais ou de interesse público. Este ecossistema acaba por ser bastante complexo, uma vez que envolve muitas entidades diferentes, pessoas, empresas e os próprios meios que armazenam informação, e muita regulamentação que nem sempre é objetiva.

Deste modo, o objetivo principal do RGPD é mitigar os riscos inerentes à partilha constante de dados pessoais, impor normas de segurança, obrigando a uma maior transparência das entidades que lidam com dados e penalizando aquelas que não cumprem com as suas obrigações. No entanto, embora seja claro que as organizações estão cada vez mais conscientes da existência do RGPD, muitas ainda não têm claro como vão fazer a sua implementação. Num inquérito feito a sessenta grandes empresas europeias, foi descoberto que apenas 10% tem maturidade no que concerne à cibersegurança e 45% necessitam de fazer investimentos significativos em ferramentas para cumprir com os requisitos do RGPD (Mikkelsen et al., 2017).

1.3 A regulação dos dados no contexto da EU através do RGPD: conceitos chave

De acordo com Schulz & Hennis-Plasschaert (2016) os dados pessoais são "*informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um*

nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. O tratamento desses mesmos dados advém de "*qualquer operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição*".

Para que todo este processo de tratamento de dados inicie, é necessário que exista uma autorização expressa e voluntária concedida pelo titular dos dados. Essa autorização, denominada de consentimento, tem que ser uma "*manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.* Continuando a seguir a linha de pensamento de Schulz & Hennis-Plasschaert (2016) o responsável pelo tratamento é "*A pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro*".

No caso de Portugal a entidade responsável pela proteção e supervisão da conformidade com o RGPD é a Comissão Nacional de Proteção de Dados (CNPD). A autoridade de controlo nacional, atualmente, é responsável também pela avaliação do impacto sobre o tratamento de dados. Primeiramente, esta autoridade tem o dever de emitir uma lista de tipos de operações de tratamento sujeitas obrigatoriamente a prévia avaliação do seu impacto sobre a proteção de

dados. De seguida e após a realização da avaliação, se o risco do tratamento ainda se afigurar elevado, pode o responsável recorrer à autoridade nacional para efeito de controlo do tratamento, nos termos do artigo 36º do RGPD. No âmbito desse controlo, a autoridade pode emitir orientações concretas, mas pode também exercer os típicos poderes de imposição de certas limitações ou mesmo de proibição do tratamento (Calvão, 2019). A autoridade de controlo é, citando Schulz & Hennis-Plasschaert (2016), *"uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51."*

O incumprimento pode também levar a sanções: "*Os Estados-Membros estabelecem as regras relativas às outras sanções aplicáveis em caso de violação do disposto no presente regulamento, nomeadamente às violações que não são sujeitas a coimas nos termos do artigo 79 a 83.o, e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas."* As sanções por incumprimento do RGPD em Portugal incluem coimas substanciais, com limites de até 20 milhões de euros ou 4% do volume de negócios global anual da empresa para infrações graves e até 10 milhões de euros ou 2% do volume de negócios global anual da empresa para infrações menos graves (art. 83º). Para além disso, os titulares de dados têm o direito de propor ações judiciais contra infratores, o processamento de dados pode ser suspenso, e as vítimas têm direito a indemnização por danos causados por violações do RGPD (art.58).

1.4 A proteção de dados no contexto do departamento de gestão de pessoas

A Gestão de Pessoas (GP) assume um papel estratégico e relevante, passando do papel tradicional de área de suporte para ser considerada como uma competência organizacional essencial, atendendo à valorização dos

colaboradores dentro de uma organização, sendo estes os principais protagonistas na consecução de resultados, quaisquer que sejam, por serem produtoras de conhecimento e inovação. Deste modo, as políticas de GP são importantes na medida em que estão alinhadas com metas da organização e fornecem as condições necessárias para que as pessoas contribuam para o alcance de melhores resultados (Demo et al., 2011). Aslanidou (2020) está em linha com esta perspetiva, afirmando que na maioria dos relatórios anuais os funcionários são considerados o maior ativo de um negócio e que o departamento de GP desempenha um papel crucial ao procurar manter os colaboradores satisfeitos e em situação regular.

Na atividade de GP, Nocker & Sena (2019) defendem que a maioria das organizações usa bases de dados para armazenar informações, bases essas que tendem a ser na *cloud*, de forma a serem de fácil utilização e permitirem maior eficiência na execução de relatórios. Estes dados armazenados incluem detalhes pessoais dos colaboradores, valores do vencimento, horários de trabalho, etc. O Departamento de Gestão de Pessoas (DGP) de uma organização é, portanto, responsável por múltiplas tarefas, tarefas essas que acarretam muitas vezes a responsabilidade de recolher, utilizar e armazenar dados pessoais.

Tal como foi referido anteriormente e tendo em conta Šišková & Lőrinczová (2020), a implementação do RGPD numa organização começa por uma auditoria interna, sendo que quando se trata de auditar os dados dos colaboradores, o processo envolve um conjunto de etapas, como definir as áreas relevantes a serem analisadas e os critérios a adotar; analisar os dados pessoais que estão armazenados nas bases de dados; analisar a sua conformidade com o RGPD; analisar as áreas de risco e por fim propor ajustes de forma a alcançar o maior grau de conformidade possível com o regulamento.

Contudo, a implementação deste "novo" regulamento tem sido um desafio para as empresas e impôs diversas mudanças a nível jurídico, técnico e

organizacional. Ao nível interno das organizações foi necessário implementar medidas técnicas e operacionais que garantissem a proteção dos dados e uma prevenção ativa do acesso não autorizado. Em primeiro lugar, a segurança física dos dados, dados esses impressos ou escritos manualmente; acesso ao arquivo; impressoras e recipientes de lixo. Em segundo, a segurança em tecnologias de informação (IT) que inclui criptografia de dados, senhas complexas, segurança técnica e medidas para monitorizar o histórico de alteração de dados e backup de dados. Por fim, a segurança pessoal, ou seja, autorização de acesso dos colaboradores ao sistema de arquivo e a devida remoção quando estes deixam de fazer parte da organização.

Nos últimos anos, o processo de transformação digital ganhou atração, abrangendo praticamente todas as áreas, incluindo empresariais. Estas mudanças particularmente intensas ocorrem nas empresas de forma a mantê-las atualizadas face à concorrência, promovendo uma maior eficiência e evolução. A multiplicidade de soluções digitais, bem como a sua crescente disponibilidade, obrigam as empresas a familiarizarem-se rapidamente com a transformação digital e a integrarem-na nos processos internos (Brodny & Tutak, 2022). Segundo estes autores, existe outra definição que considera a transformação digital como o terceiro e mais elevado nível de competências digitais alcançado, onde a utilização do digital também facilita a inovação e a criatividade e encoraja mudanças significativas no campo profissional ou do conhecimento.

O nível de alcance dos objetivos organizacionais de qualquer empresa reflete a eficácia do sistema de informação de gestão empresarial, especialmente no que diz respeito aos aspetos da gestão de recursos humanos. Aumentar a produtividade de cada colaborador reduz o custo dos serviços e melhora a qualidade da sua prestação, sendo que o rápido desenvolvimento das tecnologias de informação ajuda a resolver estes problemas fundamentais. A chave para o funcionamento estável e o desenvolvimento contínuo das empresas é um

processo simplificado de tramitação documental, sendo que os sistemas de gestão eletrónica de documentos são capazes de se adaptar às necessidades dos utilizadores ou à dimensão da empresa, o que aumenta significativamente a produtividade e a eficiência do trabalho. Contudo, para o bom funcionamento destes sistemas, é necessário a melhoria e aperfeiçoamento constante, o que permitiria satisfazer plenamente os requisitos dos utilizadores. (Khrykova & Bolsunovskaya, 2021)

No âmbito da tramitação documental por via digital, um dos temas relevantes é o que respeita à implementação de um modelo de processo de assinatura digital. Esta é um meio de validação, autenticação e segurança de documentos eletrónicos (Yadav,2018) que corresponde a um token digital que cria uma ligação entre uma entidade e um registo de dados. A validação acaba por ser o processo de certificação do conteúdo do documento, enquanto a autenticação refere-se ao processo de certificação do remetente. O processo de assinatura é implementado com a ajuda de criptografia, onde o signatário usa a sua palavra-chave privada para criar uma assinatura digital, sendo que este método é utilizado para garantir que o conteúdo original da mensagem ou documento enviado permaneça inalterado. A sua natureza variada proporcionou um mecanismo fácil, rápido, preciso e conveniente para criar, armazenar, transmitir e recuperar dados sem envolver as formalidades tradicionais em papel. Envolve benefícios como: eliminar a possibilidade de cometer fraudes (é impossível alterar a assinatura); garantir ao destinatário quem é o remetente; ser de fácil utilização; proteger a assinatura de manipulação (se a assinatura for corrompida esta perde o seu valor); ter proteção legal; e incluir um carimbo automático de data e hora.

1.5 Síntese

As tecnologias estão a evoluir num passo extraordinariamente rápido e por consequência a informação circula em questão de segundos para qualquer parte do globo. Por isso, é necessário que as normas e políticas de proteção de dados acompanhem essa evolução (Mikkelsen et al., 2017). O RGPD procura estabelecer normas para esta proteção de dados, mas é um regulamento relativamente novo e por consequência, por um lado, existem pouco estudos e, por outro, existem diversos aspetos de interpretação subjetiva, que podem levar a erros ou más interpretações das normas (Jones & Kamiski, 2020).

A área de GP lida com uma quantidade e diversidade de dados cada vez maior, o que acresce a relevância dos departamentos de gestão de pessoas nas organizações. É de grande importância e interesse de uma empresa que esses dados estejam protegidos da melhor forma possível e sempre de acordo com as normas estabelecidas (Demo et al., 2011).

Em Portugal, verifica-se a inexistência de estudos ou evidencias empíricas que façam interligação entre o RGPD e o departamento de gestão de pessoas. Grande parte dos estudos é realizada por advogados ou juristas, que estão muito centrados no regulamento em si e não na sua prática em ambiente empresarial.

É, portanto, necessário estudar a implementação do RGPD nas organizações, os desafios e vantagens que traz, e quais os pontos de melhoria. São estas as questões que guiam este estudo.

Capítulo 2

2. Método de Investigação

O tema deste estudo é a implementação do RGPD num contexto de uma organização empresarial portuguesa. Este tema é declinado nas seguintes questões que guiam o trabalho:

> **Q1:** "Quais são as fases de implementação do RGPD?"
>
> **Q2:** "Quais são os principais desafios e dificuldades na sua implementação?"
>
> **Q3:** "Quais são as principais vantagens?"
>
> **Q4:** "Quais são as oportunidades de melhoria nos processos de proteção de dados?"

Estas questões são aqui exploradas através de um estudo de caso desenvolvido numa organização empresarial portuguesa: o Grupo Nors, encabeçado pela Nors, S.A.

Num artigo publicado por Aberdeen (2013), o estudo de caso é definido como uma das estratégias de investigação mais utilizadas nas ciências sociais.

O estudo de caso é apresentado por como uma análise de eventos e factos contemporâneos num determinado contexto, sobre os quais o investigador tem reduzido ou nenhum controlo, acabando por ser completamente independente do investigador. Procura responder a questões de "como" e "porquê", permitindo uma análise profunda. Permite ainda uma abordagem dinâmica, ao explorar a evolução dos fenómenos organizacionais (Ma & Tayles, 2009).

No âmbito do estudo de caso, a recolha de dados pode ser feita através de entrevistas de diversos tipos, cruzadas com outros dados como, por exemplo, os

dados documentais. As entrevistas permitem obter informação sobre a perceção que os indivíduos têm da organização, e acabam por ser uma abordagem holística, uma vez que permitem uma visão abrangente do tema, incluindo observações e diferentes perspetivas de um meio ou contexto que vão contribuir para o enriquecimento do caso de estudo. Quanto aos dados documentais, este trabalho sustentou-se em artigos e documentos disponibilizados pela empresa (como Relatório e Contas, e o manual de procedimento de RGPD da empresa).

O estudo de caso aqui realizado tem limitações. Por um lado, o tema em análise é deveras complexo; por outro lado, o tópico da proteção de dados é tratado de forma diferente de departamento para departamento, de objetivo para objetivo e é alvo de constante mudança e atualização. Sendo assim, impõe-se uma abordagem metodológica que se aproxime à realidade.

2.1 Recolha e análise de dados

Como foi acima referido, no presente estudo foram recolhidos dados primários, quanto às entrevistas, e secundários, via informações retiradas de documentos e artigos. As entrevistas são de caracter semiestruturado, ou seja, têm uma estrutura pré-definida num guião, mas que é moldável, permitindo ao investigador explorar da melhor maneira o tema e o entrevistado (Bryman, 2016).

No que concerne a este método, é apresentado de seguida o quadro síntese, que descreve o programa de entrevistas que foi levado a cabo.

Departamento	Gestão de Pessoas	Jurídico + Consultor Externo	Auditoria e Risco	Recursos Humanos	Norshare- Serviços Partilhados
Função	Coordenadora da equipa	Advogada	Diretora e antiga DPO	Diretora	Diretora
Data da entrevista	5/01/2024	15/01/2024	22/01/2024	23/01/2024	24/01/2024
Localização	Norshare	Holding	Holding	Holding	Norshare
Duração	25 min	35 min	29 min	22 min	20 min

Tabela 1. Programa de entrevistas. Fonte: Elaboração própria

Neste trabalho, a escolha dos entrevistados foi de especial relevância, tendo sido selecionados de forma estratégica. Todos eles pertencem a diferentes departamentos e com diferentes cargos, porém, direta ou indiretamente desempenham funções que estão relacionadas com o RGPD.

Inicialmente, foi realizada a entrevista à coordenadora do departamento de Gestão de Pessoas e delegada do tratamento (RGPD). Esta colaboradora é responsável por manter o departamento funcional, tendo um profundo conhecimento de todos os processos administrativos ligados com proteção de dados. Em segundo lugar, foi feita uma entrevista a dois protagonistas, a advogada do grupo e o consultor externo (DPO), que estão responsáveis pelo RGPD nas empresas portuguesas do grupo Nors, garantindo que os processos estão em conformidade com o regulamento. Em terceiro lugar, foi entrevistada a antiga DPO (data protection officer) e atual diretora do departamento de auditoria e risco, tendo sido o pilar principal quando o RGPD foi implementado pela primeira vez na Nors, S.A.. Em quarto lugar, foi entrevistada a atual diretora dos RH e antiga gestora do DGP, que em tempos exerceu ambas as funções

cumulativamente. Durante a sua gestão no DGP, liderou a entrada e a implementação dos novos processos inerentes ao RGPD. Em quinto lugar, foi entrevistada a diretora dos serviços partilhados do grupo, (alojados na Norshare), sendo a responsável por todos os departamentos administrativos do Grupo Nors. Esta tem uma visão alargada no que toca às implicações que existiram com a chegada deste regulamento e as mudanças que aconteceram de forma a cumprir com as normas.

Para a análise destas entrevistas foi feita a transcrição parcial das mesmas, ou seja, somente das partes com relevância para as questões em análise. Esses excertos foram analisados de forma manual, sem o auxílio de ferramentas digitais, de modo a permitir captar a perceção de cada entrevistado.

Capítulo 3

3. A gestão de pessoas e a proteção de dados pessoais na Nors, S.A.

3.1 Contextualização do caso Nors, S.A.

3.1.1 Caracterização genérica do Grupo Nors

O Grupo Nors é encabeçado pela Nors, S.A. Este Grupo é uma multinacional com mais de 90 anos de existência, que assume a liderança nos setores da mobilidade pesada e equipamentos de construção, industriais e agrícolas, sendo o principal parceiro do Grupo Volvo desde 1933. Hoje em dia, detém um portefólio bastante mais diversificado, onde integra outras unidades de negócios complementares, em áreas distintas como sistemas de reciclagem, vidro para

construção ou no setor de seguros, sendo titular de 91 empresas espalhadas por diversos continentes (Sabi, 2022).

A história do Grupo iniciou-se em 1933, quando Luis Oscar Jervell se tornou o representante da marca Volvo em Portugal. Em 1949 fundou a empresa Auto-Sueco, a primeira concessionária Volvo do país. Nos anos 70, consolidou-se como uma das principais empresas do setor em Portugal, com a expansão da rede de instalações, empresas associadas e concessionárias por todo o país. Durante os anos 90, a organização continuou uma trajetória de crescimento, com a diversificação das atividades e deu início à presença internacional, primeiramente em Angola, posteriormente em Espanha. Ao longo dos anos o grupo foi aumentando a sua presença em diversas geografias – Brasil, Turquia, México, - tendo crescido sobretudo através de aquisições. Em 2013, já presente em quatro continentes e 24 mercados, a organização assumiu uma nova identidade e nome - Nors - e expandiu-se para a Europa Central.

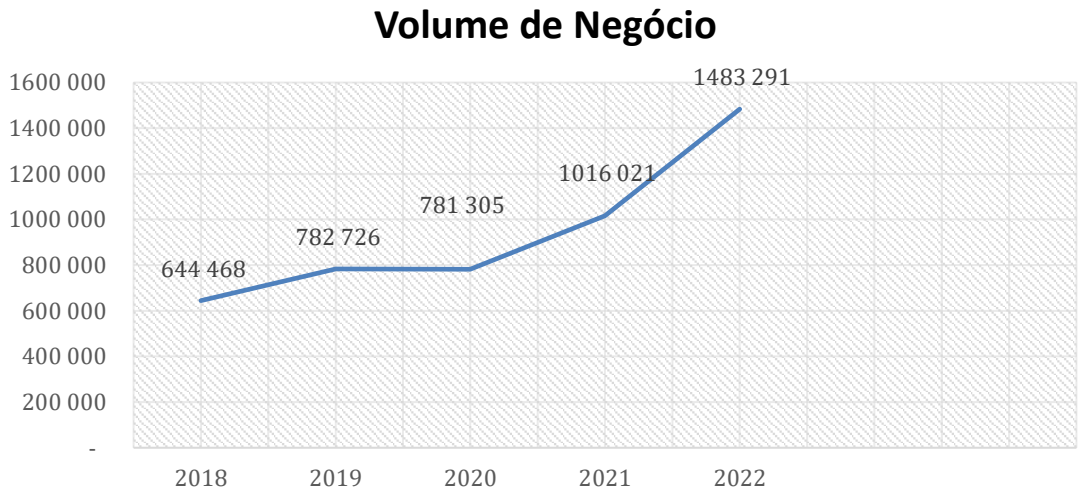
O grupo tem quatro áreas de negócios distintas como se pode ver na tabela 2: Nors Mobility, a área principal e responsável pela comercialização de veículos automóveis e veículos pesados da marca Volvo, Mazda, Renault Trucks e Kinla; a Nors Off-Road, responsável pela venda de equipamentos de construção, agrícolas e infraestruturas; a Aftermarket, especializada na distribuição e retalho de peças multimarca para automóveis, camiões e autocarros; e por fim a Nors Ventures, que explora novos empreendimentos desde a mediação de seguros até às soluções ambientais, passando pela comercialização de vidros para a construção.

Área de negócio	Marcas	Descrição	Proporção que representa no volume de negócios
Nors Mobility	Auto-Sueco, Auto-Sueco Automóveis, Galius, Kinlai	Comercialização de veículos automóveis e veículos pesados da marca Volvo, Mazda, Renault Trucks e Kinlai.	62%
Nors Off-Road	Ascendum, Auto Máquinarias, Agronew, Strongco, Agrofito	Responsável pela venda de equipamentos de construção, agrícolas e infraestruturas.	32.9%
Aftermarket	Onedrive, Civisparts, AS parts	Especializam-se na distribuição e retalho de peças multimarca para automóveis, camiões e autocarros.	4.2%
Nors Ventures	Vitrum, Amplitude, Stokon	Exploram novos empreendimentos desde a mediação de seguros até as soluções ambientais, passando pela comercialização de vidros para a construção.	0.9%

Tabela 2. Áreas de negócio do Grupo Nors. Fontes: Elaboração própria com consulta ao relatório anual de 2022

Já numa vertente mais financeira, através da consulta do Relatório e Contas de 2022, é possível verificar que o volume de negócios da Nors cresceu 130 % entre 2018 e 2022, passando de 644,468 milhões de euros para 1,483,291 milhões de

euros. Este crescimento foi impulsionado por um aumento das vendas no mercado externo, que representam a maior parte do volume de negócios. A margem bruta apresentou também um crescimento extraordinário, passando de 173,1 milhões de euros em 2021 para 264,4 milhões de euros em 2022, ou seja, um aumento de 52,7% assente sobretudo no desempenho das empresas que operam nos mercados africanos e brasileiros. Para além disso, a maior parte do volume de negócios é alcançada no mercado externo, que representa 76% das vendas, sendo apenas 24% no mercado interno (fig.3).



*milhares de euros

Gráfico 2. Volume de negócios num período de 5 anos. Fontes: Elaboração própria com consulta aos relatórios anuais de 2018 a 2022.

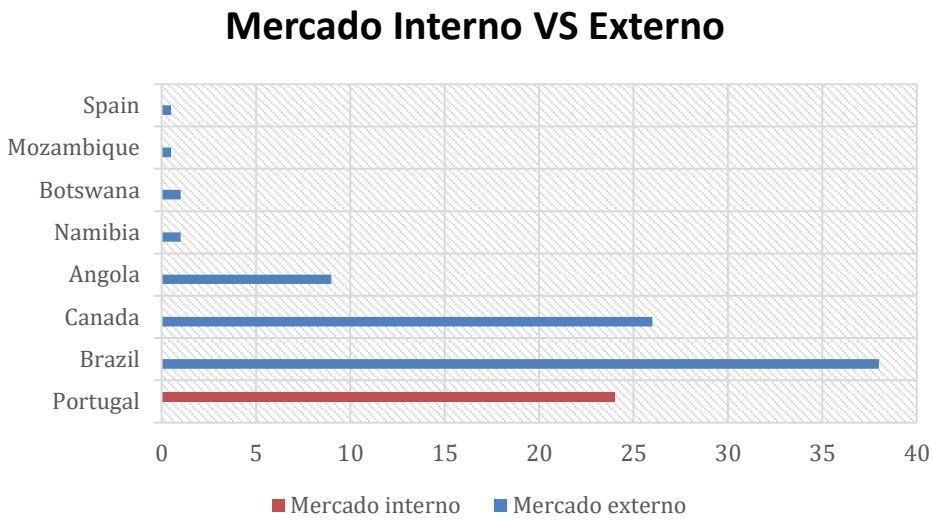
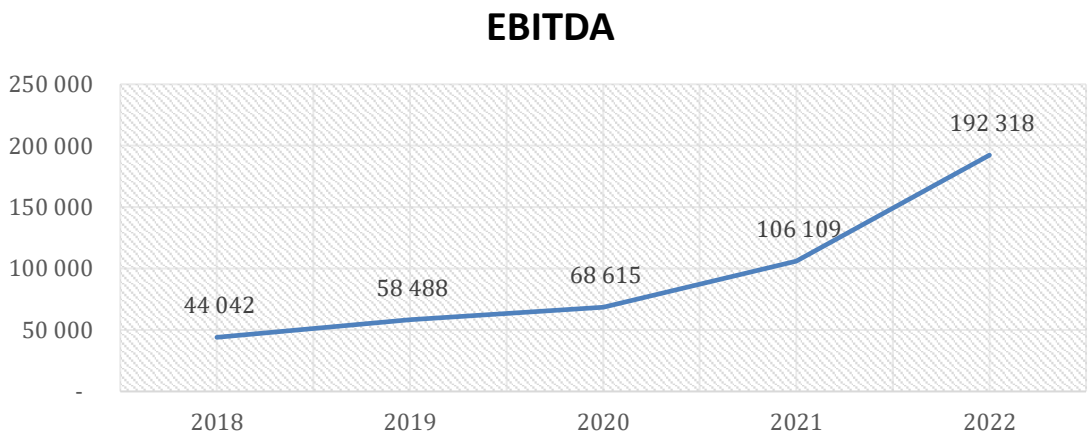


Gráfico 3. Mercado Interno VS Externo. Fontes: Elaboração própria com consulta ao relatório anual de 2022

Para além disso, o EBITDA, como é representado no fig. 4, também cresceu ao longo dos últimos 5 anos, passando de 44,042 milhões de euros em 2018 para 192,318 milhões de euros em 2022. O aumento do volume de negócios e a melhoria da eficiência operacional da empresa foram os principais fatores que desencadearam esta evolução.



*milhares de euros

Gráfico 4. EBITDA num período de 5 anos. Fontes: Elaboração própria com consulta aos relatórios anuais de 2018 a 2022

No que diz respeito ao capital humano, cresceu 90% entre 2018 e 2022, passando de 2223 para 4227 colaboradores. Este crescimento reflete a estratégia de expansão internacional com a abertura de novas lojas e oficinas em novos mercados.

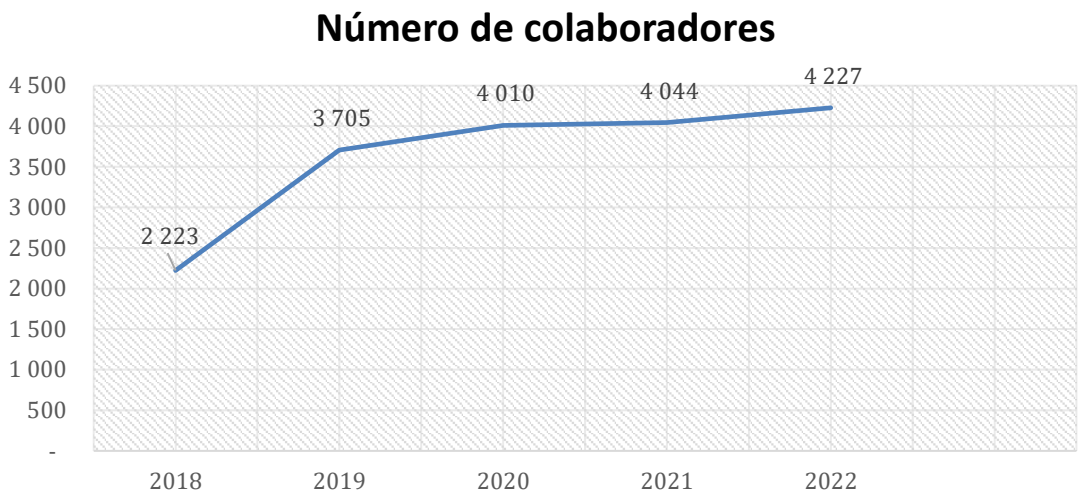


Gráfico 5. Número de colaboradores num período de 5 anos. Fontes: Elaboração própria com consulta aos relatórios anuais de 2018 a 2022

A estrutura de governo da NORS, S.A. integra a assembleia geral, o conselho de administração e o fiscal único. Existe também uma comissão de remunerações, eleita pela assembleia geral. A composição do órgão de administração é composta por administradores executivos e não executivos, sendo presidido por Tomás Jervell desde 2000. Para além disso, a estrutura de participações é dominada pela Prime Jervell Holding com 63% do capital, seguida da Cadena com 29% (Relatório e Contas,2022).

3.1.2 Caracterização genérica da estrutura de proteção de dados na organização

No que diz respeito à proteção de dados na Nors, S.A,, a partir do documento relativo aos delegados de tratamento (Nors, 2023), é possível perceber que o Grupo Nors S.A. definiu uma estrutura organizacional interna de suporte ao RGPD, sendo que esta é composta pelos elementos abaixo descritos.

O topo desta estrutura corresponde a uma Comissão Executiva, composta por 6 membros, que é responsável por orientar a estratégia em relação à proteção de dados pessoais, que inclui a definição dos objetivos, as políticas e os procedimentos necessários para cumprir as obrigações. A segunda posição é ocupada pelo DPO, sendo que este é externo, que fica responsável por atuar como ponto de contacto com a autoridade de controlo (CNPD), prestar apoio às empresas do Grupo no que diz respeito com a matéria de proteção de dados e controlar a conformidade com o regulamento. O DPO também é responsável por supervisionar o trabalho dos Gestores e Delegados do Tratamento. De seguida, é o Comité de Proteção de Dados que fornece orientação e supervisiona as atividades de tratamento de dados pessoais nas diversas empresas. Este comité é liderado pelo DPO e é composto pelo conselheiro Legal, de Tecnologia (TI) e

Gestão de Risco (GR) que prestam aconselhamento nas áreas em específico. Posto isto, existe uma divisão entre as empresas do grupo e as áreas corporativas que dão apoio a essas mesmas empresas, onde existe um gestor de tratamento, o CEO da empresa, que delega esta tarefa, normalmente, ao responsável pelo marketing. Já nas áreas corporativas, a lógica é a mesma, mas o gestor de tratamento é o diretor da área em questão de delega a função um colaborador da sua área.

Os Gestores do Tratamento representam a sua empresa em matéria de proteção de dados pessoais, sendo responsáveis por assegurar que a sua empresa cumpre as obrigações do RGPD e os delegados do tratamento são responsáveis pela

operacionalização dos princípios de proteção de dados pessoais nas respetivas empresas ou unidades organizacionais, sendo que são responsáveis por garantir

que os dados pessoais são tratados de forma lícita, leal e transparente, e que são protegidos de forma adequada.

Figura 1. Estrutura organizacional interna de suporte à proteção de dados. Fontes: Adaptado de Nors (2023)

3.1.3 Caracterização genérica da área de gestão de pessoas

O DGP é constituído por cinco pessoas, quatro técnicas e uma gestora. O departamento faz parte dos serviços partilhados do grupo, Norshare, sendo esta uma empresa que presta serviços como contabilidade, contas a receber e pagar, tesouraria, gestão de pessoas, entre outros, às restantes organizações do Grupo.

As principais funções do DGP assentam na gestão administrativa da gestão contratual: processos de admissão, renovações, caducidade e rescisões;

elaboração de contratos, minutas, documentos e comunicações e de suporte à atividade; criação e manutenção de processos individuais- cadastro de pessoal; gestão administrativa de alterações ao nível das categorias, vencimentos, benefícios e outras, nomeadamente, gratificações de desempenho e também dos horários de trabalho (construção, formalização e fixação), isenções de horário e trabalho suplementar; gestão administrativa dos descontos judiciais e penhoras de vencimento, de ferias e assiduidade e dos acidentes de trabalho, vida e saúde; elaboração de informações e estatísticas para entidades oficiais (por exemplo, o relatório único e as estatísticas para INE; contacto, esclarecimento e apoio a organismos e entidades; e manutenção e desenvolvimento funcional do sistema SAP/ RH – SF. Cada colaboradora do departimento está responsável por um conjunto de empresas do grupo e todos os processos inerentes a essas empresas. Contudo, como este trabalho está relacionado com a proteção de dados, a gestão administrativa da gestão contratual, nomeadamente, o processo de admissão é, neste caso, de maior relevância e o foco do estudo.

O processo de admissão tem início com a receção de um email com todas as informações relevantes do novo colaborador, tais como os dados do cartão de cidadão, o comprovativo de morada, e a proposta de contratação. Através destas informações é impressa e redigida uma checklist, pré-definida, para auxiliar a construção do contrato de trabalho. Depois deste contrato estar concluído, é impresso em conjunto com outros documentos, como por exemplo a declaração de IRS, o questionário médico e a política de privacidade. Estes documentos são todos anexados e enviados, através do correio interno, para o departamento de RH, onde são assinados pela diretora e pelo novo colaborador. Quando esse processo está concluído, é novamente reencaminhado para o DGP para ser tudo digitalizado e guardado na pasta individual do colaborador, em Share Point. O contrato é guardado numa pasta física e os restantes documentos que foram necessários para a admissão desse colaborador são destruídos. Só no fim desta

tarefa é que este processo está completamente concluído, sendo que são necessários 10 passos para realizar uma só admissão.

3.2 A implementação do RGPD na área de gestão de pessoas da Nors, S.A.: desafios, vantagens e oportunidades de melhoria

3.2.1 O processo de implementação do RGPD

A entrada em vigor do RPGD no grupo começou em 2018 e foi alocado à direção jurídica em parceria com a Accenture, consultora, e a Telles Abreu, sociedade de advogados. Estas idealizaram o programa de implementação deste regulamento, uma vez que se tratava de uma área muito específica e complexa, que exigia apoio externo e especializado.

O primeiro passo na implementação do RGPD numa organização consiste em realizar, numa fase inicial, uma auditoria interna. Quando se trata de auditar os dados dos colaboradores, este processo envolve várias etapas, incluindo a definição das áreas relevantes a serem analisadas e dos critérios a adotar, a análise dos dados pessoais armazenados nas bases de dados, a verificação da sua conformidade com o RGPD, a identificação das áreas de risco e, por fim, a proposta de ajustes para alcançar o maior grau de conformidade possível com o regulamento (Šišková & Lőrinczová, 2020). A advogada do grupo Nors, MP, descreveu este processo como um mapeamento rigoroso a um conjunto de áreas distintas: "*este processo começou com um minucioso levantamento de processos, registo de atividades relacionados com o tratamento de dados em todas as áreas corporativas (…) foram minuciosos a fazer o levamento*".

Após a conclusão do levantamento de todos os prossupostos inerentes ao RGPD, foi criado um sistema hierárquico com o objetivo de organizar as funções

de cada colaborador no que toca à implementação e controlo deste regulamento na organização. Relativamente ao DPO, inicialmente este começou por ser exercido por um colaborador do Grupo mas, com o decorrer do tempo foi percetível que não estavam a ser atingidas as metas necessárias. Estas envolviam modificar e, se necessário, criar procedimentos para que o RGPD fosse cumprido. Tal afirmação é percetível no discurso de MP: "*chegaram à conclusão que a independência e imparcialidade não estavam a ser rigorosamente cumpridas e precisavam de alguém cujo conhecimento não estivesse manipulado pelo conhecimento dos processos das empresas"*. Desta forma, em meados de abril de 2021 esta posição foi delegada a um advogado externo de uma sociedade de consultoria de proteção de dados.

3.2.2 Desafios percecionados

A implementação do RGPD passou por diversas dificuldades ao longo dos anos, até chegar a onde se encontra hoje. Uma das maiores adversidades encontradas foi conseguir mudar a mentalidade das pessoas, tal como reforça MP: "*Mudar a mentalidade foi difícil"*, devido ao facto de as pessoas estarem "*agarradas à simplicidade dos processos antigos*". Durante as entrevistas foi ainda mencionado por SM, atual diretora de auditoria e risco, que outra dificuldade na implementação deste regime passa por conseguir "*definir os processos que é preciso mudar", "conseguires levantar os processos todos (…) e formar as pessoas para que elas se adaptem às novas normas*". Portanto, estes desafios destacam a necessidade não apenas de identificar os processos a serem alterados, mas também de capacitar as pessoas para se ajustarem às novas normas. Isso sugere que é essencial um esforço abrangente de revisão e prática para garantir que a organização cumpre eficazmente as exigências do regime de proteção de dados.

Outra das dificuldades consiste no facto de existir uma grande variedade de empresas no grupo, B2B e B2C, levou a que a recolha de dados fosse um processo

quase interminável: *"uma base de dados gigante e com grande transferência de vendedores de um lado para o outro e eles trazem os dados dos clientes com eles*" (MP). Como se depreende do processo acima descrito, a implementação do RGPD é um processo longo, demorado e por isso geracional: "*Ainda não está feita (implementação), é um processo em constante implementação"* (DB). Ademais, a pandemia do covid-19 veio atrasar e dificultar esta transição que estava a ser feita no Grupo - *"deixou de se de fazer registos nas empresas"* (MP) - e todos aqueles pré-requisitos obrigatórios foram "*esquecidos*".

Além disso, não existe um programa que esteja preparado para lidar com as exigências e particularidades do RGPD e que auxilie os colaboradores nas tarefas. Perante isto, VS, atual diretora dos serviços partilhados da Nors, manifestou que *"faltam sistemas preparados para cumprir com o RGPD (…) pois somos obrigados a manter um determinado número de dados mas, depois há uns que tem que se ir apagando ao longo do tempo. E idealmente deveríamos ter sistemas preparados para isso e que se eliminassem automaticamente"*. SG, diretora de RH, complementa este pensamento referindo que "*o RGPD diz que, quando um colaborador sai, devíamos eliminar os dados pessoais, no entanto o nosso sistema não permite fazer isso. Ou melhor, o sistema permite a eliminação do colaborador, porém, temos de manter certos dados por questões legais*".

Um aspeto de caráter muito importante, referido por DB, prende-se com a diminuição do risco que é "*desde logo aquilo que se procura com a implementação do RGPD*". O risco, segundo a empresa, consiste na *"suscetibilidade de ocorrer um dano, neste caso o dano é de natureza reputacional, para as empresas e para o grupo caso seja de teor publico", "sendo que este pode significar quebra de confiança dos clientes e investidores na capacidade da organização em proteger adequadamente os dados pessoais recolhidos e tratados*" (Nors, 2023). Este risco vai diminuindo à medida que o grau de implementação do regulamento aumenta. Isto advém do facto de o objetivo principal do RGPD ser mitigar o risco inerente à partilha constante de dados

pessoais, impondo normas de segurança, e, como referem Flanagan & Warren, (2022), obrigar uma maior transparência da entidade que lida com dados.

Por outro lado, o dano resultante de um incumprimento do RGPD pode, não só ser de caráter reputacional, como de carácter financeiro, através de sanções, tal como referem os autores Schulz & Hennis-Plasschaert (2016).

3.2.3 Principais vantagens

Apesar da implementação do regulamento ser algo exigente e com riscos associados, acarreta consigo benefícios para as organizações que lidam constantemente com dados pessoais e sensíveis. O RGPD veio efetivamente salvaguardar essas entidades, assegurando que estas só ficam com dados estritamente necessários e quando estes o deixam de ser, são removidos, tal como explica SM: "*no fundo acabamos por não receber informação que realmente não precisamos e que por vezes até podem ser informações sensíveis de caráter confidencial*". Acrescenta ainda MG, coordenadora do DGP, que uma das vantagens do cumprimento correto do RGPD é o cumprimento legal das normas criadas para assegurar a segurança da informação confidencial, evitando assim as multas por transgressão às normas: *"A vantagem desta implementação é efetivamente o cumprimento legal e evitar que o grupo tenha coimas associadas, porque no caso de uma inspeção, se efetivamente existirem incongruência face àquilo que a lei diz, as multas são muito, muito pesadas. E isso quer para o grupo em si, quer para o departamento, não era de todo agradável imaginar que pudesse acontecer".*

Visto no prisma da eficiência, o RGPD não veio trazer melhorias para o grupo, até pelo contrário. Os colaboradores interpretam o RGPD como mais uma barreira burocrática para o sucesso da criação de uma carteira de clientes mais ampla e diversificada, porque de um momento para o outro deixaram de poder

aceder a informações cruciais para a criação de um ponto de ligação entre o comercial e o vendedor, como é possível observar nas palavras de MP: *"os colaboradores vêm o RGPD como uma boa alteração, mas também como algo que vem atrofiar os negócios. Por uma serie de razões, começou a ser sentido nas empresas B2C, uma vez que já não podiam contactar os clientes como dantes se fazia, só se podendo contactar com as pessoas que davam consentimento, esgotando-se aí o tipo de comunicação que podia ser feito. Antes, quando se enviava um email, muitos colaboradores estavam indicados em cc, e agora já não é permitido. Tudo o que é novo é visto como obstáculo e não como uma melhoria."* Por outro lado, VS, perceciona a vinda deste regulamento como algo impulsionador que fez repensar os processos, modos de trabalho e a importância dos dados pessoais, aquilo que o regulamento veio proteger: *"Acho que, apesar de tudo, fez repensar os processos e fez -nos perceber que há demasiadas pessoas, com demasiados dados pessoais, e isso também compreendo que não seja suposto. Por isso, o facto de repensarmos em cada uma das áreas os processos e percebermos o que é que pode ter ou não e restringir, cada processo, deu-nos mais segurança na proteção dos dados. Mas acho que não houve um ganho para a empresa propriamente dita, mas mais um ganho individual para cada um dos colaboradores".*

O facto dos colaboradores terem aplicado este regulamento às atividades desempenhadas na empresa, fez com que tivessem adquirido outro tipo de valências e preocupações, nomeadamente, o valor que representa um dado pessoal, a forma como este é tratado e até por vezes o que nele vem agregado, informações sigilosas, por exemplo, como explica DB: "*o minset das pessoas já começa a existir, a preocupação destas coisas, porque tudo isto está relacionado com todo o negócio, quando se fala em dados pessoais não é só o dado pessoal, este está agregado a um conjunto de informações do negocio, informações sigilosas, projetos que estão em curso…".*

3.2.4 Oportunidades de melhoria

Afunilando a análise para o DGP constata-se que apenas recentemente é que começou a ser objeto da devida atenção, tal como VS reforça "*A gestão do pessoal, apesar de estar aqui dentro dos Serviços Partilhados, reportava à Direção de Recursos Humanos, SG. E ela, sendo Diretora de RH e, ao mesmo tempo, fazendo acompanhamento da área, não tinha propriamente tempo para dedicar às exigências."* Para além disso, o departamento é caracterizado por lidar com processos extremamente administrativos, em que ainda existem muitos processos manuais e muitos documentos que, por exigência legal, têm de ser guardados em formato papel. Tal acresce ao grau de dificuldade na criação de normas e procedimentos que visam a proteção da organização e, ao mesmo tempo, a evolução dos processos: "*num departamento com muitos processos manuais, acaba por ser mais difícil serem criadas regras e procedimentos que não deem azo a que haja tanta perda de dados, além disso é um departamento que por lei tem que ter muito suporte em papel e é difícil criar um procedimento que nos venha proteger contra a perda de informação"* (MP).

Grande parte dos processos realizados no DGP é rotineira e segue um padrão que se repete. Atualmente deixa de fazer sentido esse tipo de tarefas ser feito por um colaborador, devendo passar a processar-se em formato automatizado por um programa, assegurando maior proteção, rapidez e assertividade. Neste sentido, MG descreve a falta de um sistema totalmente automatizado, que no processo de admissão anexe todos os documentos relativos ao colaborador a uma pasta, de forma automática, e quando exista um termo de contrato, permita que os documentos legalmente obrigatórios fiquem armazenados na drive, sendo os dados pessoais automaticamente apagados. Tal processo garante, assim, que as normas do RGPD estejam a ser cumpridas: *"Para mim, é na repetição de processos. (…) Em vez de termos realmente uma pasta num SharePoint com a documentação dos colaboradores, o próprio sistema de registo e de admissão do colaborador deve ter uma forma automática de eliminar os documentos que podem ser introduzidos e anexados*

durante o processo de admissão em sistema. Esse é o eixo de excelência: se tivermos um sistema otimizado em que, na fase da entrada do colaborador, anexamos todos os documentos que necessitamos e que na fase de saída, o sistema elimine X documentos, porque deixam de ser precisos e não devem ser mantidos e que passado ainda mais algum tempo, o sistema de forma automática elimine, aqueles documentos para os quais já passou o prazo legal obrigatório de manutenção pela empresa". Torna-se evidente que o DGP carece de mudança tecnológica, simplificando e melhorando certos processos acima referidos.

Capítulo 4

4. Discussão

O estudo de caso permite concluir que há significativas oportunidades de melhoria no que respeita à implementação do RGPD, sobretudo em duas áreas: na construção de uma cultura de proteção de dados pessoais, e na mudança tecnológica para maior eficiência dos processos.

Quanto ao desenvolvimento de uma cultura de proteção de dados, é essencial investir em programas abrangentes de formação e sensibilização para todos os colaboradores, enfatizando a importância da segurança da informação e os procedimentos adequados para lidar com dados sensíveis, preparando assim a mentalidade dos colaboradores.

Quanto à transformação tecnológica, deverá ser feito um investimento em sistemas de gestão de documentos e dados automatizados para simplificar e agilizar os processos de conformidade com o RGPD. Além disso, deverão ser desenvolvidos sistemas que facilitem a aplicação das normas do RGPD em todas as etapas do ciclo de vida dos dados. Devido à complexidade e ao âmbito deste processo de transformação digital, é esperado que leve tempo para ser totalmente implementado e integrado.

A Figura 2 representa dois processos diferentes: as setas a azul determinam o procedimento que é realizado atualmente no DGP; as setas a verde, por sua vez, definem a minha proposta de otimização do processo de admissão que assenta na transformação digital total do sistema.

O percurso otimizado inicia-se com a mudança da checklist para um formato somente digital e de fácil preenchimento. Posteriormente, a etapa seguinte de redação do contrato mantém-se igual ao que consta atualmente, unicamente a impressão do documento é suprimida. Na terceira etapa, os documentos são anexados ao email e de seguida são enviados para o departamento de RH para serem devidamente assinados, o que se prevê que com a otimização dure cerca de 4h. Geralmente, esta é a parte do processo mais demorada, podendo prolongar-se de 1 a 2 dias devido ao fluxo de correio interno, que só acontece 2 vezes ao dia. Ao prescindir de papel, esta etapa tornar-se-á muito mais segura e rápida com o simples enviar de email, tanto para o DRH que recebe a informação num formato mais prático para assinar como para o DGP, que obtém os documentos de forma mais segura e rápida. Este processo é viável através da assinatura digital, método que aumenta significativamente o nível de segurança, garantindo que o documento uma vez assinado não possa ser alterado e identifica o signatário que atualmente é reconhecido, à luz da legislação portuguesa, com o mesmo valor que a assinatura manuscrita tradicional.

Esta otimização, que no fundo acaba por ser a digitalização do processo, acarreta várias vantagens para a organização. Em primeiro lugar, o aumento de segurança que acaba por estar intrinsecamente relacionado com o RGPD, pois o facto da informação estar digitalmente disponível apenas para duas pessoas, o técnico de GP e a Diretora de RH, vai reduzir significativamente o risco de potenciais quebras no regulamento de proteção de dados. Em segundo lugar, a melhoria de eficiência do departamento, sendo que é possível reduzir em cerca de 45% o tempo de realização de uma admissão, como demonstra a figura 11, e

cerca de 90% o tempo de espera para que os documentos sejam assinados. Esta redução significativa do tempo de espera, deve-se ao facto de, atualmente, os documentos estarem limitados à afluência do correio interno, que só ocorre duas vezes por dia - uma de manhã e outra ao fim da tarde – porém, com o envio digital dos documentos, este problema termina. Uma outra vantagem passa pelo aumento da percentagem de sustentabilidade do departamento através da redução do uso de papel, tinteiro e energia, aproximando a organização das metas estabelecidas para a sustentabilidade. Por último, este regime acaba por representar mais um passo na direção da evolução do departamento, cujos procedimentos neste momento se encontram desatualizados do ponto de vista tecnológico. Com a entrada em vigor desta mudança tecnológica, torna-se possível implementar outro tipo de medidas que terão ainda mais impacto a nível de seguração e eficiência, fazendo com que seja de caráter imprescindível.

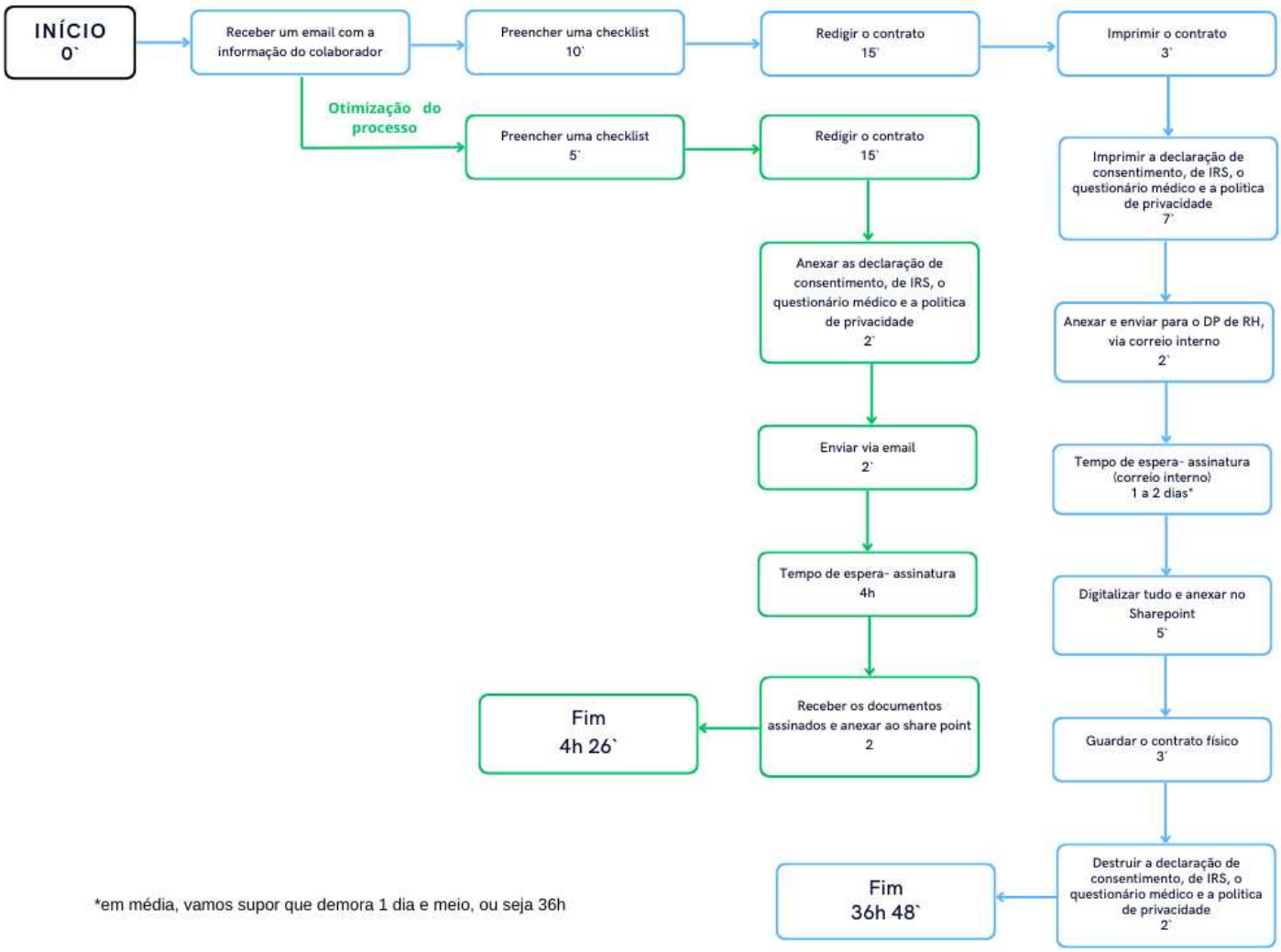


Figura 2. Fluxograma do processo de admissão de um colaborador com a digitalização. Fontes: Elaboração própria

Capítulo 5

5. Conclusão

O presente estudo tem como tema a implementação do RGPD na área de gestão de pessoas e procura responder às seguintes questões de investigação:

Q1: "Quais são as fases de implementação do RGPD?"

Q2: "Quais são os principais desafios e dificuldades na sua implementação?"

Q3: "Quais são as principais vantagens?"

Q4: "Quais são as oportunidades de melhoria nos processos de proteção de dados?"

A revisão de literatura inicial permitiu perceber que a regulamentação da proteção de dados é um tema de extrema relevância para o mundo tecnológico de hoje em dia, mas como é também um tema recente, ainda tem alguns gaps entre o que é imposto pelo RGPD, como principal normativo de proteção de dados, e o que é efetivamente exequível de se realizar. Com o avanço contínuo, as organizações estão cada dia mais próximas de alcançar um nível mais alto de implementação do RGPD, embora seja reconhecido que este processo exige um tempo considerável.

As questões foram exploradas a partir do caso da Nors, S.A. Através de 5 entrevistas realizadas a colaboradores da empresa foi possível chegar a várias conclusões. Quanto à Q1, é possível concluir que as várias fases da implementação passam por uma auditoria interna, um mapeamento de processos e registo de atividades, a criação de um sistema hierárquico de implementação e controlo e a nomeação de um DPO externo. Em resposta à Q2, identificam-se como desafios e dificuldades a resistência e a efetiva mudança na mentalidade dos colaboradores, a identificação e alteração de processos, a grande

quantidade de dados para serem tratados, o impacto da covid-19 durante a implementação das medidas, a falta de sistemas preparados para o RGPD e os riscos reputacionais e financeiros associados ao incumprimento do regulamento. Como principais vantagens, na Q3 verificam-se uma maior segurança e proteção de dados, o cumprimento legal evitando desta forma as coimas, a revisão e a melhoria de processos, a consciencialização dos colaboradores e a melhoria da confiança e reputação da organização. Por fim, quanto à Q4, os entrevistados identificam como oportunidade de melhoria, a automatização de processos, a gestão digital de documentos e a aquisição de ferramentas tecnológicas.

Mais do que apresentar respostas às questões de investigação, este TFM propõe uma melhoria num dos processos do DGP do caso analisado. Este departamento lida diariamente com dados pessoais e enfrenta uma desatualização tecnológica, o que sugere a necessidade de otimização no processo de admissão de colaboradores. Esta otimização corresponde a uma digitalização, ou seja, à passagem de todos os documentos em papel – como o contrato de trabalho, a declaração de IRS, a política de anticorrupção, entre outos – para formato digital, permitindo a validação e circulação dos documentos por meio apenas digital. Esta melhoria vem afetar o nível de proteção dos dados, minimizando consideravelmente o risco de perda ou furto durante a realização de todo o processo de admissão de um novo colaborador; uma melhoria na eficiência da tarefa, com a redução significativa do tempo de execução; e, por fim, um ganho do ponto de vista sustentável, uma vez que se deixam de utilizar os meios físicos. Ao longo do estágio não foi possível implementar esta otimização, dado a sua curta duração (5 meses), e o facto das melhorias a introduzir no processo envolverem diversas áreas que, neste momento, já se encontravam com projetos em implementação e sem margem para acumular esta mudança.

Como principal limitação a este estudo, sublinho a escassez de literatura relativa ao RGPD na área de gestão de pessoas e a falta de dados quantitativos

que, por sua vez, se sugerem para uma investigação futura. Além disso, uma proposta para trabalho futuro seria implementar a digitalização deste processo de admissão de colaboradores e analisar os impactos que teve, sobretudo quanto ao aumento do nível de segurança dos dados pessoais e do aumento da eficiência do próprio processo.

Declaração de IA generativa e tecnologias assistidas por IA no processo de redação

Durante a preparação deste trabalho, o autor utilizou o ChatGPT com o objetivo de resumir, traduzir e corrigir gramaticalmente uma parte do texto. Após a utilização desta ferramenta, o autor reviu e editou o conteúdo conforme necessário e assume total responsabilidade pelo conteúdo da publicação.

Referências Bibliográficas

Aberdeen, T. (2013). Case Study Research: Design and Methods. *Canadian Journal of Action Research*, *14*(1), 69–71.

Aslanidou, A. (2020). The impact of the general data protection regulation on human resources management in schools. *International Journal of Law and Political Sciences*, *14*, 922–929.

Brodny, J., & Tutak, M. (2022). Analyzing the Level of Digitalization among the Enterprises of the European Union Member States and Their Impact on Economic Growth. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2), 1–29. https://doi.org/10.3390/joitmc8020070

Bryman, A. (2016). *Social Research Methods* (O. U. Press, Ed.; Fifth edition, Vol. 1). Oxford University Press.

C. Thomsett, M. (2017). *The General Data Protection Regulation: A Primer for U.S.- Based Organizations That Handle EU Personal Data*.

Calvão, F. (2019). O RGPD e o Papel da Comissão Nacional de Proteção de Dados. *Revista de Direito Administrativo*, *4*, 68–70.

Chakravort, B. (2020). *Why It's So Hard for Users to Control Their Data*. Harvard Business Review. https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data

Chen, C., Frey, C. B., Presidente, G., & Benedikt Frey, C. (2022). *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally* *. https://www.oxfordmartin.ox.ac.uk/future-of-work/

Christodoulou, K., Christodoulou, P., Zinonos, Z., Carayannis, E. G., & Chatzichristofis, S. A. (2020). Health Information Exchange with Blockchain amid Covid-19-like Pandemics. *Proceedings - 16th Annual*

International Conference on Distributed Computing in Sensor Systems, DCOSS 2020, 412–417. https://doi.org/10.1109/DCOSS49796.2020.00071

Debra, J. B., & Skovira, J. R. (2017). Empowering Employees With Digital Agility: Mitigation Strategies for Information Glut. *Issues In Information Systems*, *18*, 146–157. https://doi.org/10.48009/4_iis_2017_146-157

Demo, G., Fogaça, N., Nunes, I., Edrei, L., & Francischeto, L. (2011). Políticas de gestão de pessoas no novo milênio: cenário dos estudos publicados nos periódicos da área de administração entre 2000 e 2010. *Universidade Presbiteriana Mackenzie*, *12*, 16–42.

Flanagan, A., & Warren, S. (2022). Advancing Digital Agency: The Power of Data Intermediaries. In *World Ecnonomic Forum*.

Holá, J., & Pikhart, M. (2014). The Implementation of Internal Communication System as a Way to Company Efficiency. *Business Administration and Management* , *17*(2), 161–169. https://doi.org/10.15240/tul/001/2014-2-012

Jones, M. L., & Kamiski, M. E. (2020). The GDPR: A Practical Guide for Managers. *An American`s Guide to The GDPR*, *98*(1), 93–128.

Khrykova, A., & Bolsunovskaya, M. (2021). Implementation of digital signature technology to improve the interaction in company. *E3S Web of Conferences*, *244*, 1–7. https://doi.org/10.1051/e3sconf/202124412023

Krivokapic, D., Komazec, S., & Todorovic, ivan. (2018). Impact of GDPR on Business: Focus on Data Controllers and Processors not Established within the EU. *Organization and Uncertainty in the Digital Age*, 527–539.

Ma, Y., & Tayles, M. (2009). On the Emergence of Strategic Management Accounting: An Institutional Perspective. *Accounting and Business Research*, *39*(5), 473–495. https://doi.org/10.1080/00014788.2009.9663379

Mikkelsen, D., Soller, H., & Strandell-Jansson, M. (2017). *The EU data-protection regulation-compliance burden or foundation for digitization?*

Nocker, M., & Sena, V. (2019). Big Data and Human Resources Management: The rise of Talent Analytics. *Social Sciences*, *8*(10), 1–19. https://doi.org/10.3390/socsci8100273

Nors. (2023). *Delegados do Tratamento Apresentação e Conteúdos*.

Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017). Tackling the Digitalization Challenge: How to Benefit from Digitalization In Practice. *International Journal of Information Systems and Project Management*, *5*(1), 63–77. https://doi.org/10.12821/ijispm050104

Patrick, K. (2019). DOJ Pushes Back on Idea of Consumer Control in a Federal Privacy Law. *Insedesources*.

Poosarla, S. (2022). Privacy in the Hyper-Connected World and Approach to Minimize Harms. *CSI Transactions on ICT*, *10*(1), 3–13. https://doi.org/10.1007/s40012-022-00352-z

Regulamento (UE)2016/ 679 Do Parlamento Europeu e Do Conselho, Jornal Oficial da União Europeia 1 (2016).

Sabi. (2022). *SABI Report da NORS*. www.nors.com

Schwab, K., Marcus, A., Oyola, J., & Hoffman, W. (2011). *Personal Data: The Emergence of a New Asset Class*.

Šišková, J., & Lőrinczová, E. (2020). Implementation of GDPR into Payroll Accounting in the Czech Republic. *Proceedings of the International Scientific Conference Hradec Economic Days 2020*, *10*, 804–811. https://doi.org/10.36689/uhk/hed/2020-01-090

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic Perspective Analysis of Protecting Big Data Security and Privacy. *Future Generation Computer Systems*, *98*, 660–671. https://doi.org/10.1016/j.future.2019.03.042

Yadav, M. (2018). Digital Signature. In *International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT* | (Vol. 3, Issue 6).

Apêndice A – Guião das entrevistas

Agradecimento pela disponibilidade para a realização da entrevista:

Desde já devo agradecer o seu tempo e a disponibilidade para estarmos aqui hoje reunidos para a realização desta entrevista cujo objetivo passa pelo estudo da questão de investigação do meu TFM. Seria útil para mim poder gravar a entrevista, para poder voltar a ela durante a redação do TFM. A gravação serviria apenas para este propósito, e comprometo-me a destruí-la após a aprovação do TFM. Autoriza esta gravação? Aproveito para referir que os entrevistados não serão identificados no TFM, ou seja, serão identificados pela posição que ocupam na empresa (por exemplo: gestor sénior no departamento de GP)

Apresentação breve:

Miguel,23 anos, atualmente estudante da CPBS no mestrado em Gestão. Estou a fazer o meu relatório de estágio sobre a implementação do RGPD, sendo este um tema de grande relevância na sociedade hiperconectada em que vivemos.

Pergunta de investigação:

A pergunta de investigação está focada nos benefícios e desafios na implementação do RGPD no grupo Nors, mais especificamente no departamento de GP. Este trabalho procura perceber também as grandes vantagens na otimização de diversas tarefas relacionadas com dados pessoais, sendo que a evolução tecnológica é um dos principais fatores para que esta otimização se torne possível.

Antes de começarmos, será que podia fornecer me algumas informações, de modo a conhecer melhor quem é que está desse lado.

- Qual é o seu nome?
- Qual é a sua posição na empresa?
- Há quanto tempo trabalha nesta empresa e quais foram as posições que teve anteriormente? E antes de trabalhar nesta empresa, que experiências profissionais teve?

Entrevista base:

- Quando é que foi implementado o RGPD no grupo?

- Como foi a implementação do RGPD no dp GP?
    - Como foi planeada a implementação do RGPD? Quem fez parte da equipa? Houve alguma consultoria externa? De quem e por que motivo? Qual o envolvimento da gestão de topo neste processo?
    - Quais foram as principais fases de implementação? Como decorreram? Quais os principais desvios face ao que estava planeado? Como se adaptaram?
    - Quem foram os principais responsáveis pela implementação? Como estavam distribuídas as respetivas competências ou tarefas?
    - Quais foram os principais desafios e obstáculos enfrentados?

- Quais foram as principais vantagens da implementação do RGPD?
    - Quais foram os principais ganhos (em termos de segurança, privacidade e conformidade ou outros)?
    - Quais foram os principais ganhos em termos de eficiência?

- Quais foram as principais aprendizagens da implementação do RGPD? O que mudariam, caso fossem implementá-lo agora?

- Quais são os pontos que poderiam ser melhorados na implementação do RGPD?
  - Quais são as principais áreas onde o dp de GP ainda pode melhorar a sua eficiência e produtividade na gestão de dados pessoais?

- Até que ponto é que a tecnologia pode ajudar na otimização do processo de admissão de novos colaboradores?

Perguntas de follow-up

- Pode dar-me um exemplo específico de um desafio que enfrentou na implementação do RGPD e de como o resolveu?

Conclusão

- Agradecer ao entrevistador pelo seu tempo e colaboração. Perguntar se pode mais tarde colocar questões que entretanto surjam, e como deve fazê.o (email ou presencial). Reiterar que a gravação – caso autorizada – serve apenas para efeitos de redação do trabalho e será destruída após aprovação do TFM, e que o entrevistado não será identificado no TFM

Apêndice B – Email tipo para participação nas entrevistas

Assunto: Convite para Colaboração em Pesquisa Académica sobre a Implementação do RGPD no departamento de GP

Boa tarde (Nome),

Espero que esta mensagem a encontre bem. O meu nome é Miguel Rouxinol, e sou estudante do mestrado em Gestão na Católica Porto Business School. Atualmente, estou a estagiar no departamento de GP do Grupo e ao mesmo tempo estou a realizar o meu trabalho final de mestrado relativamente à implementação do RGPD no Grupo mais especificamente do departamento de GP.

A pesquisa visa compreender o RGPD, o departamento de GP e uma proposta de implementação para otimizar um dos processos no departamento.

O meu método de estudo são entrevistas a diversos colaboradores de departamentos diferentes com o objetivo de reunir diferentes perspetivas de forma a conseguir realizar o estudo mais verídico possível.

A colaboração envolveria uma entrevista que seria conduzida de acordo com a sua disponibilidade. Se estiver interessado em participar ficaria grato se pudéssemos agendar uma reunião!

Agradeço antecipadamente pela sua consideração e espero contar com a sua participação neste importante projeto de pesquisa.

Atenciosamente,

Miguel Rouxinol