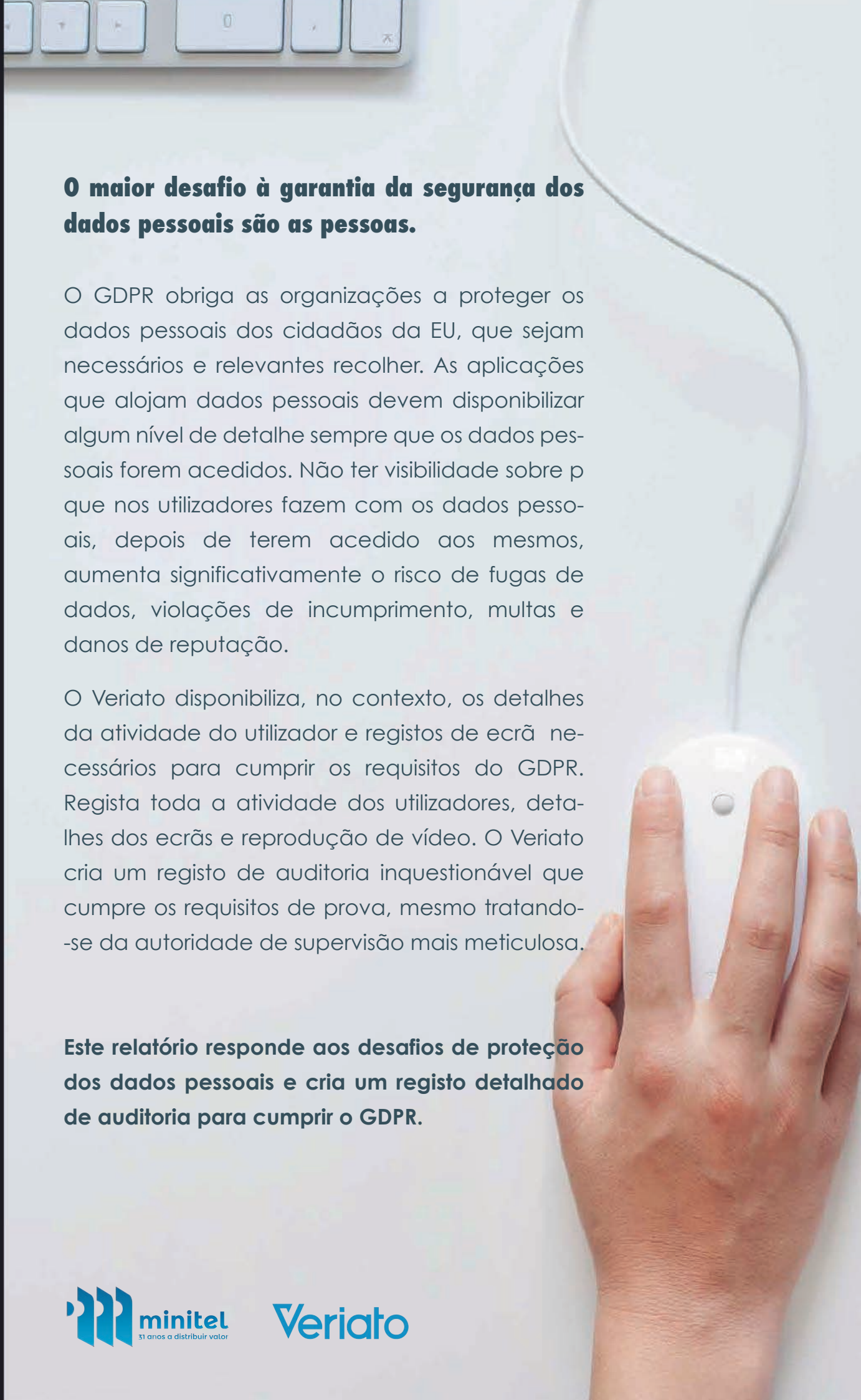
DEMONSTRAR A CONFORMIDADE COM O GDPR

minitel
31 anos a distribuir valor

Veriato



O maior desafio à garantia da segurança dos dados pessoais são as pessoas.

O GDPR obriga as organizações a proteger os dados pessoais dos cidadãos da EU, que sejam necessários e relevantes recolher. As aplicações que alojam dados pessoais devem disponibilizar algum nível de detalhe sempre que os dados pessoais forem acedidos. Não ter visibilidade sobre p que nos utilizadores fazem com os dados pessoais, depois de terem acedido aos mesmos, aumenta significativamente o risco de fugas de dados, violações de incumprimento, multas e danos de reputação.

O Veriato disponibiliza, no contexto, os detalhes da atividade do utilizador e registos de ecrã necessários para cumprir os requisitos do GDPR. Regista toda a atividade dos utilizadores, detalhes dos ecrãs e reprodução de vídeo. O Veriato cria um registo de auditoria inquestionável que cumpre os requisitos de prova, mesmo tratando-se da autoridade de supervisão mais meticulosa.

Este relatório responde aos desafios de proteção dos dados pessoais e cria um registo detalhado de auditoria para cumprir o GDPR.

minitel
31 anos a distribuir valor

Veriato

Introdução

O Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, em vigor a partir de 25 de Maio de 2018, vai alterar a forma de fazer negócios de muitas empresas, no mundo inteiro, envolvendo cidadãos da União Europeia. O conceito de dados pessoais do GDPR é muito abrangente. De acordo com o regulamento, os dados pessoais são informação relativa a uma pessoa singular identificada ou identificável (titular dos dados), que possa ser usada para, direta ou indiretamente, identificar uma pessoa, como por exemplo um nome, uma fotografia, um endereço de email, número de identificação, dados de localização, detalhes bancários, posts em redes sociais, informação médica ou um endereço IP de computador. São estes dados que devem ser protegidos.

Existem multas para a fuga até 4% da faturação anual da empresa ou 20 milhões de euros, o que for maior. Evitar estas penalidades depende apenas da capacidade da organização demonstrar o processamento e os controlos de segurança adequados para prevenir uma fuga de dados. Caso exista uma fuga de dados, tem de ser obrigatoriamente reportada às autoridades em 72 horas. As organizações precisam de um registo de auditoria que disponibilize o detalhe necessário para documentar a importância da fuga.

Assim sendo, o que é necessário é um ferramenta que permita ter uma visibilidade completa sobre qualquer ação dos utilizadores, com acesso aos dados pessoais – todas as aplicações utilizadas, webpages visitadas, gravações copiadas, ficheiros arquivados, printscreens e páginas impressas. Só assim o responsável pelo tratamento dos dados sabe verdadeiramente se os dados pessoais foram acedidos e utilizados de forma adequada.

Mas, o cumprimento do GDPR não é apenas uma batalha técnica: é colmatado com políticas administrativas e processos que, em conjugação com a tecnologia, garantem que os utilizadores estão treinados, que o acesso aos dados pessoais foi corretamente concedido, que a utilização e o tratamento são adequados e que o cumprimento pode ser demonstrado.

Os desafios do GDRP para as várias partes interessadas

As responsabilidades do GDPR são imputadas às organizações e à nova função - encarregado de proteção de dados - Data Protection Officer (DPO), as diversas partes interessadas na organização têm diferentes necessidades em torno do objetivo de cumprirem o GDPR:

Precisa de uma estratégia proativa, que influencie pessoas, processos e tecnologias e que garanta o alinhamento dos requisitos do GDPR para proteger os dados pessoais.

Não se pode dar ao luxo de permitir gastar tanto no incumprimento devido a uma fuga. Prefere gastar o orçamento em medidas preventivas, do que medidas de reposta à fuga.

Quer um plano definido que demonstre de forma fácil e rápida a conformidade.

Deseja garantir que os processos de dados pessoais, atividades e sistemas estão conformes com o GDPR.

Pretende que os dados pessoais continuem seguros e quer ter forma de saber se os dados pessoais estão a ser utilizados abusivamente.

IT Manager – Precisa de perceber onde é que os dados residem, assim como eventuais redundâncias. Necessita de ferramentas de visibilidade de acordo com a abrangente definição de dados pessoais do GDPR, independentemente da aplicação.

É necessário uma tecnologia que responda eficazmente e com um custo acessível aos requisitos do GDPR, monitorizando os processos que envolvam dados pessoais, alinhando com políticas e processos já estabelecidos, com visibilidade sobre como os dados pessoais são utilizados, disponibilizando o contexto em volta, demonstrando a conformidade ou a extensão da fuga.

O Veriato ajuda a ultrapassar os desafios do GDPR

O Veriato ajuda todo o tipo de empresas a cumprir eficazmente as obrigações relacionadas com a avaliação do risco, garantindo que existe a proteção apropriada e demonstrando que o acesso é adequado, através da disponibilização do contexto em que a fuga ocorre. Fá-lo registando e disponibilizando o acesso a atividades do utilizador – tanto nas aplicações usadas para processar os dados pessoais, como qualquer outra aplicação – combinando uma reprodução robusta de ecrã e vídeo. Políticas customizadas e alertas ajudam as empresas a definir responsabilidades adequadas aos seus ambientes únicos.

Esta solução pode ser usada para examinar e avaliar se a segurança de um processo, ou acesso aos dados pessoais é feito, por todos, de forma adequada, reproduzindo as ações envolvidas na fuga de dados. Toda os dados referentes à atividade são pesquisáveis, fazendo com que seja mais fácil para o DPO, auditor, equipas de segurança ou mesmo o IT, encontrar comportamentos suspeitos, podendo reproduzir o antes, o durante e o depois do tratamento da atividade em questão. Os alertas informam a empresa sobre o comportamento suspeito dos utilizadores, minimizando os riscos de fuga. Os relatórios podem ser produzidos em minutos e não requerem a utilização de recursos críticos.

O Veriato auxilia ao cumprimento de vários artigos do regulamento, utilizando a sua visibilidade sobre ações especificas dos utilizadores, relacionadas com acesso e tratamento dos dados pessoais.
As secções seguintes descrevem como o Veriato pode ajudar no cumprimento de requisitos específicos do GDPR.

ARTIGO 24

Deveres do responsável pelo tratamento de dados

O responsável pelo tratamento no GDPR tem de garantir que os dados são apenas acedidos e usados para tratamento relacionado com as finalidades do negócio e com o tipo de operações que levam a cabo. O Veriato pode ser usado para monitorizar a interação do utilizador com os sistemas de dados específicos e aplicações relacionadas com o GDPR.

Como pode o Veriato ajudar relativamente às responsabilidades do controlador?

Comprovar que o tratamento que realiza é apropriado, conforme com o GDPR (Parágrafo 1)

O Veriato regista qualquer ação do utilizador, disponibilizando ao DPO o detalhe de atividade usado para comprovar que o tratamento está a ser executado de acordo com o GDPR.

ARTIGO 25

Proteção de dados por defeito, desde a sua concepção

DPO Encarregado de Proteção de Dados responsável por assegurar uma segurança adequada aos sistemas e aplicações utilizadas para processar os dados pessoais, assim como a sua implementação e tratamento.

- O Veriato disponibiliza uma visibilidade sem limites sobre os acessos, aplicações utilizadas, informações visualizadas e o que está a ser feito. Todos os factores são testados para verificar se a proteção de dados está implementada corretamente. Proteção de dados na génese do tratamento, de um produto ou serviço que implique a utilização de dados pessoais.

Como pode o Veriato responder a alguns princípios de concepção do GDPR?

Validar os princípios de proteção de dados (Parágrafo 4)

Os dados da atividade podem servir como base de verificação de que existe a proteção necessária no tratamento de dados. Revendo como os utilizadores acedem e processam os dados, permite perceber e comprovar rapidamente se as medidas de proteção estão a ser executadas.

Assegurar a inacessibilidade dos dados (Parágrafo 2)

Através da monitorização dos acessos dos utilizadores aos dados pessoas, o Veriato analisa mais claramente sempre que os dados pessoais estão a ser acedidos, de forma a garantir que esses dados estão acessíveis aos utilizadores internos adequados, por defeito.

ARTIGO 30

Registo de atividades de tratamento

O GDPR exige um registo de todas as atividades de tratamento. A capacidade de registar, reportar e reproduzir a atividade do utilizador, disponibiliza às empresas detalhes específicos no contexto das atividades tratadas. Políticas personalizadas podem ajudar os processadores e controladores a gerir esta informação e disponibilizar relatórios fáceis de compreender.

ARTIGO 32

Segurança no tratamento

À semelhança da maioria dos padrões de segurança na indústria, o GDPR exige assegurar, avaliar e validar a segurança no tratamento de dados pessoais. Conciliando com a avaliação do impacto do risco prevista no Artigo 35, este artigo procura garantir um nível de segurança adequado ao risco no caso de uma violação de dados pessoais na empresa.

Como pode o Veriato ajudar na definição e manutenção da segurança?

Garantir uma segurança regular e contínua (Parágrafo 1d)

Responder à necessidade de avaliação regular das medidas de controlo técnico e organizativas para a segurança no tratamento de dados, disponibilizando uma forma abrangente de acesso e revisão da atividade do utilizador. O detalhe da atividade é fornecido tanto para as aplicações relacionadas com o processamento, como para qualquer aplicação que possa potencializar roubo, exposição ou outro tipo de utilização abusiva dos dados pessoais.

Avaliação do risco no processamento (Parágrafo 2)

Quer seja acidental ou intencional, os detalhes da atividade ajudam na avaliação do nível de segurança adequado e dos riscos pelo tratamento em particular devido à destruição, perda e alterações acidentais ou ilícitas e divulgação e acesso não autorizado dos dados pessoais, trans-

Validação do processo adequado (Parágrafo 4)

Monitorização e auditoria da utilização da aplicação, com possibilidade de notificar o DPO, ou outro staff apropriado, do acesso a dados pessoais através de alertas ou reporting. Este detalhe de auditoria pode ser utilizado para validar que o acesso e tratamento dos dados pessoais não ocorre sem aprovação do responsável pelo tratamento, como é exigido.

ARTIGO 33

Notificação da violação dos dados à Entidade Supervisora

O GDPR exige a notificação de uma fuga de dados em 72 horas após a ocorrência. Isto significa que a organização precisa de monitorizar permanentemente as fugas de dados pessoais. Para além disso, se ocorrer uma violação, o GDPR exige que as empresas definam a extensão da fuga, reportem e descrevam as suas consequências. Se a explicação for inadequada pode ter como consequência uma multa. O Veriato ajuda tanto na deteção da atividade potencial de fuga, como também disponibiliza detalhes da atividade no caso de ter ocorrido uma violação.

Como pode o Veriato ajudar deteção de fugas de dados pessoais?

Detectar potenciais riscos de fuga

Os analíticos de comportamento do utilizador do Veriato (UEBA) identificam os utilizadores, demonstrando a ameaça potencial de fuga através da monitorização e análise de alterações de comportamento e comunicação. Tanto o responsável IT, como o DPO, podem ser notificados de qualquer risco potencial e do momento em deve ser efectuada uma análise à atividade do utilizador.

Deteção de fugas potenciais

Monitorizar, detectar e alertar para atividades especificas do utilizador, que o responsável IT considere inapropriadas. Isto pode ser baseado na utilização da aplicação, pesquisa de palavras-chave e ou noutros factores.

Definir/descrever a natureza da violação de dados (Parágrafos 3a e 5)

Se ocorrer uma fuga, a atividade do utilizador pode ser reproduzida em vídeo pelo Veriato, em contexto com as ações que aconteceram antes, durante e após a fuga. Estes detalhes podem ser utilizados como parte integrante da documentação que o responsável do tratamento tem de disponibilizar à Autoridade de Controlo, no caso de violação de dados pessoais, para verificação do cumprimento.

ARTIGO 35

Avaliação do Impacto

Uma avaliação do impacto tem subjacente a exposição aos riscos no processo ou a confirmação que o processo protege completamente os dados pessoais.

A monitorização da atividade única do Veriato, ajuda a avaliar o estado corrente das operações e a sua conformidade com o GDPR.

ARTIGO 41

Supervisão dos códigos de conduta aprovados

Periodicamente, as autoridades de supervisão podem rever as políticas, processos e documentação da organização verificando a sua conformidade com o GDPR. O registo da atividade do utilizador do Veriato pode disponibilizar o detalhe necessário a qualquer auditoria ou conduta do utilizador.

Como pode o Veriato ajudar na supervisão da conduta?

Rever periodicamente o seu funcionamento (Parágrafo 2b)

Como parte da revisão periódica, a autoridade de supervisão (CNPD) precisa de auditar os procedimentos atuais do processamento de dados pessoais. O Veriato, não só capacita as autoridades de supervisão na verificação da atividade registada do utilizador nos sistemas que contenham dados pessoais protegidos, como também em qualquer aplicação, disponibilizando uma visibilidade sem limites das ações que envolvam tratamento de dados pessoais.

Demonstrar a conformidade ao GDPR com o Veriato

O GDPR é, sem sombra de dúvida, a legislação com maior impacto em qualquer negócio com clientes na União Europeia. Em ultima instância, o GDPR foi desenhado para assegurar a privacidade dos dados pessoais. No caso do acesso e tratamento de registos pessoais ser efetuado por alguém que tem uma necessidade legítima e que só utilize essa informação para a atuação e finalidade da sua função/organização, a empresa está em conformidade.

No entanto, os utilizadores com acesso a registos pessoais utilizam diariamente esse acesso e torna-se praticamente impossível dizer se e quando a sua organização deixa de estar em conformidade.
Por exemplo, o acesso a um registo pode parecer apropriado, contudo o cortar e colar essa mesma informação num documento separado e guardado num disco cloud já, certamente, não o é. Isto significa que a sua organização precisa de monitorizar supervisionar e registar todas as atividades dos utilizadores, independentemente da aplicação.

O Veriato ajuda na conformidade com os requisitos do GDPR, disponibilizando de forma idêntica ao responsável IT, DPO, equipas de segurança e autoridades de supervisão de forma idêntica uma visibilidade completa sobre qualquer ação levada a cabo pelos utilizadores dessa organização. O Veriato tem as soluções que ajudam a analisar o risco, testar a segurança no tratamento de dados e rever a atividade, num esforço para identificar fugas e o seu enquadramento.