ManageEngine

Tudo o que você precisa saber e fazer para estar em conformidade com o Regulamento Geral de Proteção de Dados da UE

Índice

Introdução

Os aumentos no número, na escala e no custo das violações de dados fizeram com que os governos de todo o mundo promulgassem leis de conformidade rigorosas para proteger os dados pessoais dos cidadãos. A Europa não foge à regra. Desde 2012, a Comissão Europeia vem criando outras proteções que podem melhorar os métodos de processamento de dados, aprimorar sua segurança e harmonizar a proteção de dados confidenciais em todas as nações europeias.

Com muitas alterações nas regras de proteção de dados existentes, o novo Regulamento Geral de Proteção de Dados (GDPR) está chamando mais atenção. A estrutura da GDPR da UE é complexa de implementar, com suas novas políticas de responsabilização, procedimentos de notificação de violação e regras rígidas para fluxos de dados internacionais.

Este guia destaca as principais alterações, desafios e planos de ação que as organizações devem adotar para garantir a conformidade com o regulamento GDPR.

Alterações, requisitos e planos de ação

GDPR não tem fronteiras

A GDPR é uma lei global de proteção de dados que se estende além das empresas que operam apenas na UE. Qualquer organização que vise consumidores neste local, processe os dados pessoais de seus cidadãos ou monitore o comportamento dos titulares de dados da UE deve estar em conformidade com os requisitos da GDPR.

Requisitos:

- É hora de rever as estruturas e políticas de segurança das empresas. As organizações que não operam na UE, mas que lidam com seus dados, deverão tomar medidas para cumprir a GDPR.
- As organizações que operam na UE e estão em conformidade com a atual lei de proteção de dados também devem rever sua estrutura de segurança, para garantir que estão cumprindo os rigorosos requisitos doa GDPR.

Os planos de ação

- Se a sua organização fornecer bens ou serviços ou monitorar o comportamento de cidadãos da UE, você precisará estar em conformidade com os requisitos da GDPR a partir de 25 de maio de 2018.
- Reveja suas políticas de segurança e certifique-se de tomar as medidas adequadas, conforme descrito abaixo, ao gerenciar dados pessoais.
- Elabore notas de privacidade adequadas e outros documentos que possam ser usados para obter consentimento explícito e claro das pessoas para processar seus dados pessoais. Se você já tiver esses documentos, considere revisá-los de acordo com o novo regulamento.
- Monitore as medidas técnicas e organizacionais tomadas para garantir a privacidade e a segurança dos dados pessoais coletados.
- Se necessário, indique funcionários que possam monitorar os processos de dados e que sejam responsabilizáveis pela segurança de dados pessoais e confidenciais.

Escopo de dados pessoais ampliado

O novo regulamento amplia a definição de dados pessoais e dados pessoais confidenciais.

De acordo com a GDPR, os dados pessoais são "qualquer informação relacionada a uma pessoa física identificada e identificável". Ele também inclui "identificadores online", como endereços IP e identificadores de cookies.

Além de definir dados pessoais, a GDPR categoriza alguns dos dados pessoais como confidenciais. De acordo com ela, dados pessoais confidenciais são "quaisquer dados relacionados à origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, vida sexual ou de saúde e dados genéticos e biométricos".

Os novos requisitos também impõem que as organizações obtenham consentimento válido dos "titulares dos dados" antes de processar seus dados pessoais.

Desafios:

- Essa definição ampla de dados pessoais e a inclusão do "identificador online" forçam as organizações que lidam com analítica de dados, análise comportamental, publicidade e mídias sociais a respeitarem a GDPR.

Os planos de ação

- Defina o escopo dos dados com os quais sua organização lida.
- Se os dados se encaixarem na definição da GDPR de "dados pessoais", prepare uma nota de privacidade ou documento que solicite consentimento explícito e claro de indivíduos para processamento adicional de dados.
- Se você já estiver procurando consentimento para processar os dados, considere revisá-los e analisá-los de acordo com os novos requisitos de conformidade.

Princípios de proteção de dados redefinidos

O princípio de proteção de dados que forma a espinha dorsal dos requisitos da GDPR permanece o mesmo que aquele declarado na Lei de Proteção de Dados, o regulamento de conformidade anterior, com mais alguns elementos adicionados.

Os seis princípios de proteção de dados descrevem que os dados pessoais e os dados pessoais confidenciais devem ser

- Processados de forma justa, legal e transparente.
- Coletados para fins específicos, explícitos e legítimos e não devem ser processados de maneira incompatível com os objetivos acima mencionados. O arquivamento suplementar dos dados para interesses públicos ou fins científicos, históricos ou estatísticos não será incompatível com os objetivos iniciais.
- Adequados, relevantes e limitados ao que é necessário em relação à finalidade para a qual ele é processado.
- Preciso e atualizado. Devem ser tomadas medidas para apagar ou corrigir dados pessoais imprecisos.
- Mantida de forma que permita a identificação de titulares de dados por não mais do que o necessário para os fins para os quais ela é processada. Só pode ser arquivado por um período mais longo se o arquivamento servir a interesses públicos ou fins científicos, históricos ou estatísticos. Além disso, as organizações devem tomar medidas técnicas para salvaguardar os direitos e a liberdade das pessoas.
- Processado com medidas técnicas e organizacionais adequadas que garantam a segurança apropriada, incluindo proteção contra processos ilegais, perda acidental, destruição ou danos.

A nova GDPR descreve requisitos rígidos de responsabilização que fazem com que os controladores de dados a) sejam responsáveis por garantir que os princípios de proteção de dados estejam em vigor e b) demonstrem que a organização está em conformidade com o regulamento GDPR.

Requisitos:

- Além de cumprir os princípios de proteção de dados, as empresas devem definir claramente sua função no processamento (ou seja, controladores ou processadores) e assumir suas responsabilidades de acordo com o novo regulamento.

  As organizações devem revisar seu fluxo de auditoria de dados para cumprir os novos requisitos de responsabilização do regulamento GDPR.

- As empresas devem adotar uma nova abordagem baseada em risco se estiverem processando dados pessoais de risco substancial. Os controladores de dados devem realizar avaliações de impacto à proteção de dados (DPIAs), para determinar o risco associado aos dados pessoais mesmo antes de serem processados. A DPIA também permite a identificação e mitigação de violações em um estágio inicial, para reduzir os danos causados pelos custos que podem ocorrer.
- Quando um projeto que lida com dados pessoais está sendo iniciado, as organizações devem adotar uma abordagem de privacidade por projeto, para reduzir o risco de violações de dados.

Os planos de ação

- Documente todas as informações relacionadas ao processamento de dados, incluindo:
  - Quais tipos de dados pessoais serão coletados.
  - Como serão coletados, usados, transmitidos e armazenados.
  - Como serão protegidos contra exposição em cada etapa.
- Além de documentar informações, inclusive onde os dados estão sendo armazenados e quem os detém, as empresas devem monitorar constantemente atividades como:
  - Quem acessa dados pessoais.
  - Com quem os dados estão sendo compartilhados.
- Monitore continuamente o arquivo ou a pasta onde os dados estão armazenados, para identificar instantaneamente e reportar quaisquer tentativas de acesso não autorizadas ou ilegais.
- Mantenha um registro de por quanto tempo os dados devem ficar armazenados. E, no decorrer do armazenamento, certifique-se de que os dados estejam criptografados e protegidos contra violação.

Responsabilidade e prestação de contas

Todas as organizações que processam dados pessoais ou confidenciais atuam como um controlador ou como um processador. Para garantir a responsabilização, a GDPR atinge o equilíbrio certo entre as funções, tornando-as igualmente responsáveis por estarem em conformidade.

Controladores de dados

- De acordo com a GDPR, "os controladores são qualquer entidade que, isoladamente ou em conjunto com outras pessoas, determina como e por que os dados pessoais são processados".
- Os controladores são responsáveis por:
  - Revisar todas as atividades de processamento de dados.
  - Manter a documentação relevante de todas as atividades de processamento de dados.
  - Conduzir avaliações de riscos à proteção de dados para processos de alto risco.
  - Implementar a proteção de dados por projeto e por padrão.
  - Nomear processadores de dados e definir instruções sobre como processar os dados.
  - Notificar as autoridades em caso de violação de dados.

Processadores de dados

- De acordo com a GDPR, um processador de dados é "qualquer pessoa (que não seja o funcionário do controlador de dados) que processa os dados em nome do controlador de dados".

  Os processadores de dados fazem o seguinte:

  - Processam dados somente mediante instrução documentada do controlador.
  - Empregam medidas de segurança e organizacionais para evitar violações de dados.
  - Excluem todos os dados pessoais no final do processamento e mediante instrução do controlador.
  - Mantêm um registro por escrito das atividades de processamento realizadas em nome dos controladores.
  - Designam um Diretor de Proteção de Dados (DPO) quando necessário.
  - Notificam os controladores imediatamente depois que uma violação de dados tenha ocorrido.
  - Fornecem todas as informações necessárias aos controladores para demonstrar a conformidade e permitir que auditorias sejam conduzidas pelo controlador.

Requisitos:

- As empresas devem revisar e analisar cuidadosamente seus contratos de processamento de dados existentes para cumprir os requisitos de responsabilização que foram alterados. Todos os novos contratos devem cumprir os novos requisitos da GDPR.
- Os processadores e controladores devem rever suas políticas de segurança, auditoria e violação de dados para cumprir os novos requisitos da GDPR.
- As organizações devem manter registros de ações tomadas para evitar violações de dados.

Os planos de ação

- Mantenha um registro claro do fluxo de dados dentro da organização, ou seja, como estão sendo coletados, acessados, compartilhados e quem os mantém.
- Tenha políticas de segurança que possam evitar violações de dados. Isso inclui:
  - Monitorar a rede da organização para detectar qualquer anomalia.
  - Rastrear os comportamentos dos usuários, especialmente usuários privilegiados que têm acesso ao processamento de dados pessoais.
  - Fazer auditoria do arquivo e da pasta em que os dados pessoais estão sendo armazenados. Obtenha informações instantâneas sempre que houver tentativas de acesso inapropriadas ou não autorizadas a dados pessoais.
  - Garantir medidas organizacionais e técnicas adequadas para proteger a rede da empresa contra ataques e ameaças.

Notificação de violação de dados

A GDPR define a violação de dados pessoais como "uma violação da segurança que cause destruição, perda, alteração, divulgação ou acesso a dados pessoais sem autorização".

Isso explica que uma violação de dados é mais do que apenas a perda de dados. O regulamento também força as organizações a relatarem violações de dados "sem atraso indevido e, quando possível," em 72 horas.

Requisitos:

- As empresas devem ter um procedimento adequado de relatório de violação interna.
- As organizações devem realizar revisões da cadeia de suprimentos e auditorias regulares para garantir que estão cumprindo os novos requisitos de segurança.
- As empresas devem implantar um sistema técnico e de segurança adequado que facilite a detecção instantânea de violações de dados. O sistema também deve fornecer informações detalhadas para acelerar a resposta ou conter a violação em um estágio inicial.

Os planos de ação

- Identificar os indicadores de comprometimento (IoCs) que causam violações de segurança na rede e preparar políticas de segurança para defendê-las.
- Implantar sistemas de segurança, como firewalls e IDS/IPS, que podem ajudar a evitar ataques de segurança.
- Considerar a implementação de soluções de segurança para organizações que possam detectar, alertar e relatar violações instantaneamente. Além disso, as soluções devem ser capazes de alertar em tempo real sempre que ocorrerem incidentes ou tentativas de violação.
- Adotar políticas de segurança que ajudem a garantir a integridade dos dados identificando as seguintes ações não autorizadas:
    - Acesso ou tentativas de acesso
    - Exclusão
    - Compartilhamento
    - Copiar ou tentar copiar dados pessoais
- Monitorar o comportamento de usuários privilegiados (ou seja, usuários que têm acesso a dados pessoais), para identificar atividades anormais em caso de roubo de identidade e denunciá-las imediatamente.

Os direitos dos titulares dos dados

Qualquer ação que você possa executar com dados é considerada um processamento. No entanto, a GDPR define limites rígidos sobre o que as organizações podem ou não fazer com as informações pessoais que coletam.

Direito de ser informado: Começa a partir do ponto de coleta de dados. As organizações devem informar aos titulares dos dados que as informações coletadas deles serão processadas de maneira transparente e justa, por meio de uma nota de privacidade. Além disso, é necessário que as empresas obtenham consentimento claro e válido dos titulares dos dados para processar suas informações pessoais por meio de um documento de consentimento estabelecido em termos simples.

Direito de acesso: Indivíduos ou titulares de dados devem ter o direito de acessar suas informações pessoais a qualquer momento. Por esse requisito, a GDPR garante que os indivíduos tenham o direito de verificar e validar se suas informações estão sendo processadas de forma justa.

Direito à retificação: Se os indivíduos sentirem que seus dados pessoais estão incompletos ou imprecisos, eles têm o direito de solicitar à empresa que os corrija. Quando uma solicitação de retificação tiver sido solicitada, é responsabilidade do controlador fornecer informações sobre as ações tomadas mediante solicitação, sem atraso indevido aos indivíduos envolvidos.

Direito à restrição do processamento de dados: Quando o processamento de dados é restrito, o controlador pode apenas armazenar os dados pessoais e não pode executar nenhum tipo de processamento. As pessoas podem restringir o processamento de dados se:

- Os dados estão imprecisos ou incompletos.
- Os dados forem processados ilegalmente.
- O controlador não tem mais nenhum motivo (de acordo com os princípios de proteção de dados) para processar os dados pessoais.

Direito à portabilidade de dados: Os indivíduos, a qualquer momento, sem obstáculos, podem obter seus dados e transferi-los para outro controlador para processamento. Esse direito permite que as pessoas movam, copiem ou transfiram dados pessoais facilmente de um ambiente para outro de forma segura.

Direito de ser esquecido: A GDPR concede direitos totais aos indivíduos para solicitar a exclusão ou remoção de seus dados pessoais. A solicitação de eliminação de dados pode ser solicitada sob estas circunstâncias:

- Quando o armazenamento de dados pessoais já não for necessário em relação à finalidade para a qual foram originalmente coletados ou processados.
- Quando o indivíduo retira o consentimento para o processamento de dados.
- Quando o titular dos dados levanta uma solicitação para interromper o processamento de dados devido ao processamento ilegal a uma violação de dados.
- Se os dados precisarem ser apagados para cumprir uma obrigação legal.

Os planos de ação

- Elabore um formulário de busca de consentimento ou uma nota de privacidade adequada que possa obter consentimento claro e explícito de indivíduos para processar dados pessoais.
- Documente as técnicas e os fluxos de processamento de dados para que você possa fornecer aos indivíduos quando eles os buscarem por meio de seu direito de acesso.
- Tome medidas técnicas para apagar dados pessoais automaticamente após o cumprimento de sua finalidade.
- Enquanto os dados estiverem sendo armazenados, certifique-se de que sua integridade seja preservada criptografando-os.
- Documente as informações de criptografia para fornecê-las aos titulares dos dados, se necessário.

Penalidades para a violação da conformidade

Quando as organizações não estão em conformidade com a GDPR ou violam seus requisitos, os administradores podem impor uma penalidade de até *10 milhões de euros ou 2% do total de rotatividade anual mundial da empresa no ano financeiro anterior,* o que for maior. Os controladores e os processadores de dados são responsáveis por essa enorme multa quando as condições abaixo são violadas:

- Princípios fundamentais de proteção de dados
- Condições de processamento de dados não pessoais
- Condições para consentimento
- Condições de processamento de dados pessoais confidenciais
- Direitos dos titulares dos dados

O comissário responsável pela proteção de dados, que impõe a multa, toma em consideração a natureza e intensidade da violação, as medidas de mitigação tomadas, as medidas técnicas e organizacionais implementadas e muito mais para decidir o montante da penalização.

Cumprimento dos requisitos de conformidade com a GDPR nas soluções de segurança de TI da ManageEngine

O portfólio de soluções de segurança de TI da ManageEngine tem uma ampla variedade de ferramentas que ajudam as organizações a cumprir a GDPR. Temos em nossa suíte:

- o **Log360**, uma ferramenta SIEM abrangente, que ajuda as empresas a detectar violações de dados, garantir a segurança dos dados pessoais armazenados e rastrear o acesso aos dados pessoais, confirmando os requisitos de responsabilização.

- o **File Audit Plus,** uma ferramenta de auditoria e monitoramento de arquivos em tempo real, que ajuda a rastrear quaisquer alterações críticas no arquivo e na pasta em que os dados pessoais são armazenados.

Como nossas soluções ajudam a cumprir os requisitos da GDPR

- **A medida técnica e organizacional para defender ou atenuar violações de segurança:** A implantação do Log360 e do File Audit Plus pode ser a medida técnica que as organizações adotam para defender ou atenuar violações de segurança. Essas soluções têm a capacidade de monitorar as atividades de todos os dispositivos e usuários em sua rede, além de relatar anomalias aos administradores instantaneamente. O profissional de segurança pode, então, investigar o incidente com extensos relatórios e, se o incidente for considerado uma violação de segurança (ou tentativa de violação), ele pode tomar medidas imediatas para contê-lo num estágio inicial.

- **Auditoria de dados:** O recurso de monitoramento de integridade de arquivos em tempo real do File Audit Plus monitora continuamente as alterações nos dados críticos. Ele também fornece extensas informações sobre quem acessou os dados, quando eles foram acessados e de onde. Esse relatório detalhado ajuda a fornecer informações aos titulares sobre acessos e monitora os fluxos.

- **Condução de trilhas de auditorias:** A poderosa capacidade de pesquisa de logs do Log360 ajuda a realizar análises forenses com facilidade. É um dos requisitos da GDPR descobrir a causa-raiz da violação ou tentar corrigi-la instantaneamente. Nossa solução pode ajudar a encontrar a causa-raiz pesquisando terabytes de dados de logs em minutos. Também fornece uma opção para exportar os resultados da pesquisa como um relatório forense para que eles possam ser enviados aos DPOs. Além disso, a consulta de pesquisa pode ser convertida em um perfil de alerta para atenuar futuros ataques de segurança do mesmo tipo.

- **Cumprimento dos requisitos PIA/DPIA:** Os extensos relatórios e perfis de alerta do Log360 detectam imediatamente quaisquer anomalias na rede e tentativas de violação de segurança. Isso ajuda a conter a violação de dados em um estágio inicial e a minimizar os danos e os custos que poderiam incorrer de outra forma, cumprindo, assim, os requisitos PIA/DPIA da GDPR.

- **Requisito de notificação de violação:** O Log360 envia alertas por e-mail ou SMS em tempo real sobre violações de dados aos administradores. Isso os ajuda a relatar a violação a funcionários superiores sem qualquer atraso indevido. Essa solução vem com mais de 600 perfis de alerta predefinidos que são baseados em vários IoCs. Isso ajuda a detectar as tentativas de violação instantaneamente, sem muito esforço. Além disso, a solução também oferece uma opção para criar perfis de alerta personalizados para atender às necessidades de segurança interna.

Soluções de segurança de TI da ManageEngine para a conformidade com a GDPR

Log360

Uma solução de SIEM integrada que combina o ADAudit Plus e o EventLog Analyzer, as duas ferramentas de auditoria mais avançadas, para resolver todos os desafios de gerenciamento de logs e segurança de rede. Frustre ataques internos de segurança, defenda sua rede contra ataques externos, proteja informações confidenciais e atenda ao exigente crescimento da conformidade.

Faça o teste grátis de 30 dias | Saiba mais

FileAudit Plus

Uma solução de SIEM integrada que combina o ADAudit Plus e o EventLog Analyzer, as duas ferramentas de auditoria mais avançadas, para resolver todos os desafios de gerenciamento de logs e segurança de rede. Frustre ataques internos de segurança, defenda sua rede contra ataques externos, proteja informações confidenciais e atenda ao exigente crescimento da conformidade.

Faça o teste grátis de 30 dias | Saiba mais

ManageEngine

Sobre a ManageEngine

A ManageEngine fornece as ferramentas de gerenciamento de TI em tempo real que capacitam a equipe para atender às necessidades da organização relacionadas a serviços e suporte em tempo real. Em todo o mundo, mais de 60.000 empresas estabelecidas e emergentes – incluindo mais de 60 por cento das empresas da Fortune 500 – confiam nos produtos da ManageEngine para garantir o desempenho ideal de sua infraestrutura de TI crítica, incluindo redes, servidores, aplicações, desktops e mais. A ManageEngine é uma divisão da Zoho Corp. com escritórios em países do mundo inteiro, entre eles Estados Unidos, Reino Unido, Índia, Japão e China.

Sobre a autora

Subhalakshmi Ganapathy atualmente trabalha como Analista Sênior de Marketing de Produtos para soluções de Segurança de TI na ManageEngine. Ela tem conhecimento profundo de segurança da informação e do gerenciamento de conformidade, ministra orientação estratégica para empresas sobre gerenciamento de eventos e informações de segurança (SIEM), segurança de rede e privacidade de dados.

Entre em contato com a Subha pelo e-mail subhalakshmi.g@manageengine.com.

Ligação grátis:

EUA: +1 888 720 9500 Reino Unido: 0800 028 6590 Austrália: +1 800 631 268

China: +86 400 660 8680 Internacional: +1 925 924 9500

Ou

Visite www.manageengine.com/log-management para saber mais sobre o Log360.

Visite www.fileauditplus.com para saber mais sobre o File Audit Plus.