Informatica

white paper

Recomendações sobre como lidar com o "D" em GDPR

SOBRE A INFORMATICA

A transformação digital muda expectativas: melhor serviço, entrega mais rápida e com menos custos. As empresas devem mudar para continuar competitivas, e a solução está nos dados.

Como líder mundial em gerenciamento de dados em nuvem empresarial, estamos preparados para ajudar você a liderar de maneira inteligente em qualquer setor, categoria ou nicho. A Informatica oferece a perspectiva para que você se torne mais ágil, aproveite novas oportunidades de crescimento ou invente coisas novas. Estamos 100% focados em todos os tipos de dados para oferecer a versatilidade de que você precisa para prosperar.

Convidamos você a explorar tudo o que a Informatica tem a oferecer — e estimular o poder dos dados para impulsionar sua próxima revolução com inteligência.

Índice

1. Resumo executivo 4

2. Contexto 5

2.1 Contexto geral e implicações potenciais 5

2.2 A quem a GDPR é pertinente? 6

2.3 O que torna a GDPR um desafio de uma perspectiva de dados? 6

2.4 Tipos de dados potencialmente no escopo 6

3. Pontos de entrada, requisitos de capacidade e casos de uso de tecnologia 7

3.1 Pergunta de ponto de entrada: Onde estão todos os nossos dados potenciais em escopo? 8

3.2 Pergunta de ponto de entrada: Como nossos dados pessoais estão sendo utilizados? 9

3.3 Pergunta de ponto de entrada: Como gerenciamos os dados dos titulares dos dados? 10

3.4 Pergunta de ponto de entrada: Como proteger dados e impedir o acesso não autorizado? 11

4. Parceiros 12

5. Conclusão 12

6. Aviso legal 12

1. Resumo executivo

A partir de maio de 2018, a Regulamentação Geral de Proteção de Dados (GDPR) da União Europeia entrará em vigor, proporcionando maior proteção aos dados pessoais. A GDPR aplica-se a qualquer organização estabelecida na UE e a qualquer organização (em qualquer parte do mundo) que processe os dados pessoais de titulares dos dados da UE, por oferecer produtos ou serviços ou ao monitorar ou acompanhar suas atividades. Essa regulamentação poderia ter um impacto significativo para muitas organizações e na forma como elas gerenciam dados pertencentes a clientes, consumidores, parceiros, funcionários e outros "titulares dos dados", em que um "titular dos dados" é um indivíduo. A GDPR afeta o armazenamento, o processamento, o acesso, a transferência e a divulgação de registros de dados de um indivíduo, além de ter algumas penalidades potencialmente muito graves para violações.

A GDPR exigirá que muitas organizações compreendam como usam os ativos de informação atuais e futuros para incorporar esses novos requisitos de privacidade de dados e melhorar os direitos de privacidade dos cidadãos. Para muitos, as mudanças associadas às práticas de gerenciamento de informação exigirão uma avaliação completa das capacidades atuais e futuras referentes à manipulação de dados. Este documento examina como a análise desses requisitos ajuda a compreender os desafios de dados e o rumo que as organizações poderiam tomar para suas iniciativas de GDPR.

Para auxiliar o entendimento, este documento examina algumas das perguntas mais comuns que muitas organizações fazem em sua jornada rumo à GDPR. Chamamos essas perguntas de perguntas de ponto de entrada. Para ajudar a responder a cada pergunta de ponto de entrada, definimos um conjunto de requisitos de capacidades que consideramos importante e, alinhado a cada capacidade, há um caso de uso de tecnologia que esclarece como cada capacidade pode ser desenvolvida. A tabela abaixo mostra como esses itens estão todos relacionados.

Pergunta de ponto de entrada	Requisito de capacidade	Caso de uso de tecnologia
Onde estão todos os nossos dados potenciais em escopo?	Descoberta de dados confidenciais e análise de riscos	Detecção e proteção
Como nossos dados pessoais estão sendo utilizados?	Interpretação de políticas	Governança de dados corporativos
Como gerenciamos os dados dos titulares dos dados?	Gerenciamento de dados pessoais	Correspondência de dados e caso de uso de vínculo
Como protegemos os dados e impedimos o acesso não autorizado?	Habilitação de controles de segurança de dados	Detecção e proteção

Há também exemplos em que os requisitos, como a captura de consentimento e o gerenciamento, podem abranger vários requisitos de capacidade e casos de uso de tecnologia; portanto, as organizações precisam de uma compreensão clara das complexidades potenciais envolvidas.

Embora a GDPR apresente muitos desafios, ela oferece muitas oportunidades para a utilização de dados. Este documento descreve as abordagens de caso de uso potencial e se baseia em nossa vasta experiência no gerenciamento de dados para ajudar as organizações a enfrentar esses desafios e, ao mesmo tempo, adotar soluções inovadoras de gerenciamento de dados, governança e funcionalidades de segurança para maximizar seus programas de conformidade. A Informatica oferece soluções de software inovadoras e integradas para automatizar, proteger e controlar os dados, e essas soluções podem fornecer, rapidamente, suporte às organizações em suas iniciativas de GDPR.

2. Contexto

2.1 Contexto geral e implicações potenciais

A digitalização da sociedade está avançando a um ritmo acelerado, com quase todas as organizações aproveitando o poder dos dados para melhorar as decisões de negócios, envolver clientes e parceiros e promover processos de negócios transformadores. A Comissão Europeia reconheceu que grande parte dos dados que estão sendo criados, coletados, processados e armazenados são, de fato, dados pessoais, que podem revelar informações extensas sobre os titulares dos dados da UE.

A regulamentação existente referente à proteção de dados não necessariamente aquietou as preocupações com a proteção e a segurança dos dados pessoais. A diversidade de regulamentações referentes à proteção de dados nos Estados membros da UE frustra os titulares dos dados, com 90% indicando que gostariam de ver a mesma regulamentação de proteção de dados aplicada em toda a UE — seja qual for o local onde seus dados são armazenados ou processados.*

Consequentemente, a GDPR foi promulgada para proteger melhor os direitos fundamentais dos cidadãos à privacidade na era digital e trazer à atenção preocupações relativas à diversidade das leis de proteção de dados.

Com início em maio de 2018, a GDPR exigirá que muitas organizações gerenciem e protejam com mais eficiência os dados de clientes, cidadãos, funcionários e outros. Este regulamento aplica-se aos titulares dos dados da UE, independentemente de nacionalidade ou residência, a fim de prescrever princípios e regras para a proteção de dados pessoais.

Com a GDPR sendo uma regulamentação baseada em "princípios", isto significa que as organizações devem considerar quais obrigações elas precisam, ou não, cumprir, considerando as circunstâncias únicas de seus negócios e do uso de dados. Portanto, muitas organizações precisarão criar uma interpretação desses princípios para ajudá-las a orientar e conduzir suas iniciativas de GDPR.

A GDPR exigirá que muitas organizações compreendam melhor como utilizarão seus ativos de informação atuais e futuros para seguir esses novos princípios de privacidade de dados. Isto terá um impacto sobre as pessoas, os processos, a tecnologia e as práticas e políticas de gerenciamento de dados de muitas organizações.

Violações da regulamentação poderiam ter penalidades financeiras significativas para muitas organizações, dependendo do tipo e da escala da violação. Multas de até 20 milhões de euros ou 4% do faturamento total mundial de uma organização, o valor que for mais alto, poderiam ser aplicadas.

* http://ec.europa.eu/justice/data-protection/reform/index_en.htm

2.2 A quem a GDPR é pertinente?

A conformidade com GDPR apresenta várias dimensões e não está limitada pela geografia física; organizações da América do Norte, Ásia e de outros continentes devem segui-la, caso armazenem e processem titulares dos dados da UE. Atualmente, os dados pessoais são manipulados por organizações que lidam diretamente com consumidores (B2C), organizações que lidam com outras organizações (B2B), bem como empresas de processamento de dados dedicadas. As organizações que processam dados sobre titulares dos dados da UE precisarão compreender por completo seus requisitos de conformidade, não importa qual país suas operações ou seus data centers estejam fisicamente localizados.

2.3 O que torna a GDPR um desafio de uma perspectiva de dados?

Para muitas organizações, existem desafios de dados distintos em relação à GDPR. A conformidade com GDPR implica controle e governança de dados pessoais, onde quer que estejam em uma organização. No entanto, a proliferação de dados pelas organizações e seus ecossistemas de negócios pode tornar seu gerenciamento um grande desafio. Tendências importantes, como um aumento na diversidade de dados e uma mudança para a computação baseada em nuvem, aumentam os desafios de segurança e gerenciamento de dados, criando um cenário de TI altamente dinâmico. Para demonstrar esses desafios, fornecemos algumas perguntas relativas à GDPR que muitas organizações estão tendo dificuldades em responder:

- Onde, em qualquer organização e em seu ecossistema, estão todos os dados no escopo e relevantes aos quais os princípios da GDPR se aplicam? Esses dados correm algum risco?
- Como as organizações controlam seus dados em seus ecossistemas operacionais?
- Como uma organização define e gerencia todos os seus ativos de dados relevantes para ajudar a garantir que todas as políticas e todos os procedimentos necessários sejam aplicados e impostos?
- Onde, em qualquer organização, são mantidos todos os registros de dados no escopo relevantes aos quais os princípios da GDPR se aplicam? Como eles podem ser identificados e vinculados?
- Como uma organização captura e gerencia o consentimento fornecido por um titular dos dados? Como uma organização pode gerenciar mudanças na escolha de consentimento do titular dos dados ou gerenciar a definição de consentimento?
- Como uma organização pode responder com eficiência e eficácia às solicitações de acesso, ao direito ao apagamento e às solicitações de portabilidade dos titulares dentro dos prazos exigidos?
- Como a organização controla o acesso aos dados relevantes? Os dados de privacidade são removidos quando não são necessários para a função ou atividade da organização?

2.4 Tipos de dados potencialmente no escopo

Outro desafio potencial é como as organizações respondem aos tipos de dados que mantêm. Neste contexto, definimos tipos de duas maneiras:

1. Um tipo de entidade de dados
2. Um tipo de tecnologia que gerencia o tipo de entidade de dados

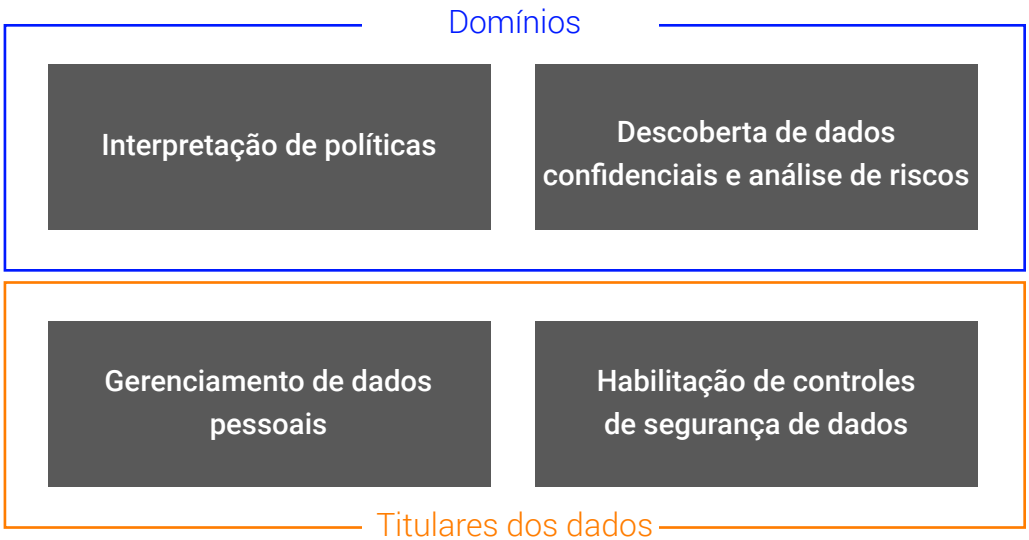
A maioria das informações dos titulares dos dados se enquadraria em um ou mais tipos de entidade de dados, bem como em um ou mais tipos de tecnologia. O diagrama abaixo mostra alguns exemplos de tipos de dados e tecnologia potenciais, que podem ser aplicados aos dados da GDPR no escopo:

ENTIDADE DE DADOS	TECNOLOGIA				
• Cliente • Cliente • Segurado • Beneficiário • Contato • Funcionário • Empresa contratada • Voluntário • Visitante • Outra(s)	• Estruturados • Semiestruturados • Não estruturados	• On-line • Perto da linha • Off-line • Backup	• Digital • Físicos • Combinados	• Explícitos • Implícitos • Combinados	• Internos • Externos

Esses diferentes tipos podem obrigar as organizações a considerar abordagens, métodos e tecnologias muitos diferentes para captura e gerenciamento de ativos de dados da GDPR no escopo.

3. Pontos de entrada, requisitos de capacidade e casos de uso de tecnologia

Para ajudar a melhorar a compreensão e a conscientização, bem como o planejamento de atividades, a Informatica identificou várias perguntas fundamentais de ponto de entrada que destacam alguns dos desafios de dados mais comuns da GDPR. Esses pontos de entrada costumam ser acionados por perguntas simples que podem exigir que as organizações considerem cuidadosamente as pessoas, os processos e a tecnologia necessários para produzir as respostas. Para ajudar a responder a essas perguntas, descrevemos as capacidades potenciais necessárias, bem como alguns casos de uso de tecnologia que fornecem as capacidades necessárias. As capacidades necessárias são estruturadas em grupos; o diagrama abaixo mostra como esse agrupamento funciona e a relevância de cada grupo.



Essas capacidades encontram-se em duas áreas chamadas domínios e titulares dos dados.

Domínios refere-se aos domínios dos dados dos titulares dos dados. Essa área ajuda a gerar insights sobre a descoberta e o gerenciamento do domínio, que são utilizados na definição de escopo e no fornecimento de uma visão organizacional dos dados.

Titulares dos dados refere-se aos dados dos titulares dos dados reais em um nível transacional. Essa área ajuda a gerar insights sobre o gerenciamento de dados pessoais, que são usados para apresentar respostas e insights referentes ao titular.

3.1 Pergunta de ponto de entrada: Onde estão todos os nossos dados potenciais em escopo?
Contexto: Em geral, os dados estão distribuídos em muitos sistemas, aplicativos e fontes em toda uma empresa. Isto é especialmente verdadeiro para organizações maiores e para aquelas que cresceram por aquisição. Devido às funções que os titulares dos dados da UE podem desempenhar em uma organização (cliente, fornecedor, parceiro, funcionário, etc.), é pouco provável que os dados pessoais ficarão restritos a um departamento ou sistema. As organizações com sistemas de TI mais diversificados não deverão apenas considerar os dados em aplicativos básicos, mas também em planilhas, bancos de dados locais e soluções de Big Data.

Capacidades necessárias: Descoberta de dados confidenciais e análise de risco é a capacidade de descobrir dados em uma ampla gama de soluções de tecnologia e utilizá-los, juntamente com outras fontes de informação, como as quantidades de dados reais e a proliferação de dados, para criar uma pontuação de risco para os dados. A pontuação de risco ajuda as organizações a compreender onde os dados de maior risco estão armazenados, de modo que quaisquer requisitos potenciais de correção ou controle de segurança possam ser priorizados com base em um risco. O acompanhamento da pontuação de risco ao longo do tempo mostra se as atividades de correção ou controle melhoraram a posição de risco dos dados. Em apoio aos propósitos legais, o consentimento pode ser necessário, de maneira que as capacidades, como a linhagem de dados, ajudem as organizações a identificar novos repositórios de dados pessoais para ajudar na compreensão das mudanças potenciais em uso.

Caso de uso de tecnologia: A descoberta de dados confidenciais e a análise de riscos podem ser caracterizadas como sendo um caso de uso de detecção e proteção, com foco na detecção. Essas são as principais capacidades para gerar insights sobre onde os dados confidenciais no escopo estão armazenados e para onde eles proliferam, com insights analíticos sobre o risco dos dados. As capacidades típicas que poderiam ser aplicadas a esse caso de uso incluem:

- **Definição da política de dados:** Definições de negócios e de TI, dados vagos e conflito entre políticas
- **Descoberta automatizada de dados:** Encontrar os dados confidenciais no escopo relevantes, primeiro com a aprovação e, em seguida, monitoramento contínuo, classificação de dados e integração de sistemas de suporte
- **Proliferação de dados:** Onde estão os dados? Para onde eles vão? Novas fontes?
- **Pontuação de risco dos dados:** Baseado na movimentação de dados + proliferação + acesso + volume, priorização mais planejamento, histórico e monitoramento da pontuação ao longo do tempo
- **Proteção de dados:** Identificar os pontos em que o acesso a dados precisa de restrições, quais dados deveriam ser anonimizados, onde a criptografia deveria ser aplicada e a visualização de dados com base no tempo, na localização e na função

Soluções de tecnologia: O **Informatica Secure@Source** poderia ser utilizado para ajudar a descobrir a localização de dados no escopo, classificá-los, monitorar a proliferação de dados e atribuir pontuações de risco. O acompanhamento ao longo do tempo mostra como as mudanças influenciam positiva ou negativamente os esforços em direção à conformidade.

Benefício: Gerar insights não apenas sobre a localização dos dados, mas também classificar os dados de acordo com o risco.

3.2 Pergunta de ponto de entrada: Como nossos dados pessoais estão sendo utilizados?
Contexto: Nosso mundo está passando por uma transformação digital que afeta todos os setores. O aumento dos dados gerados, coletados e analisados é uma clara tendência global, e uma porcentagem significativa dos dados pode ser atribuída a dados pessoais de indivíduos. Conforme os dados se proliferam em uma organização, a propriedade, o controle e o gerenciamento desses dados torna-se um desafio cada vez maior. Assim como muitas formas de conformidade regulamentar, a conformidade com GDPR será mais bem alcançada por meio de uma abordagem à governança de dados que abrange toda a empresa.

Capacidades necessárias: A interpretação de políticas é uma capacidade de capturar a compreensão das políticas de negócios e de tecnologia, responsabilidades, processos, termos de dados e modelos lógicos e físicos. Fundamentalmente, é também o local em que a compreensão do ambiente técnico está vinculada à compreensão do ambiente de negócios. Esse vínculo fornece às organizações uma visão holística das informações sobre seus domínios de dados no escopo e constitui uma parte integrante de uma abordagem para o gerenciamento de seus ativos de dados.

Caso de uso de tecnologia: A interpretação de políticas poderia ser caracterizada como sendo um caso de uso de governança de dados corporativos. Essas são as principais capacidades para fornecer uma visão ascendente e descendente do gerenciamento organizacional dos dados, com vínculos entre a visão de informações de negócios e de TI. Os requisitos típicos que seriam aplicáveis a esse caso de uso incluem:

- **Definição da política:** Definições de negócios e de TI, documentação em todos os níveis operacionais da empresa, modelos de processo e de dados lógicos e físicos
- **Responsabilidades:** Quem possui os dados, quem utiliza os dados e quais funções têm a responsabilidade pela qualidade e segurança?
- **Definição de termos e processos:** Processos de negócios, principais entidades de dados, atributos, sistemas, qualidade e controles, normalização, definições de consentimento de negócios
- **Processo de mudança:** Processo regido para definições, processo regulado para mudança, governança do processo
- **Vínculo a artefatos:** Vínculo de artefatos lógicos a físicos, linhagem de dados técnicos e corporativos, incorporação da qualidade dos dados

Soluções de tecnologia: Adotar soluções de governança de dados corporativos que permitem que funções de negócios e de TI trabalhem em conjunto em busca do objetivo comum da governança de dados. Soluções, como o **Informatica Axon Data Governance**, foram especificamente projetadas para unir visões de dados corporativos e de TI e criar o vínculo entre os ativos de dados lógicos e físicos.

Benefício: Contribuição fácil e rápida de todos os especialistas no assunto para definir os processos, as políticas e as entidades de dados que a organização tem para desenvolver rapidamente uma capacidade de governança holística de dados para os dados no escopo.

3.3 Pergunta de ponto de entrada: Como gerenciamos os dados dos titulares dos dados?
Contexto: Como resultado direto do uso diversificado de dados em ambientes complexos de TI, a criação de uma visão única de todas as informações de titulares dos dados individuais é um grande desafio. Esse desafio decorre do fato de que diferentes sistemas usam mecanismos muito diferentes para armazenar e indexar dados. Sem uma visão completa dos dados de titulares dos dados individuais e de como eles são gerenciados, armazenados ou processados em uma organização, a conformidade com GDPR será um grande desafio, especialmente no que diz respeito aos direitos de dados individuais.

Capacidades necessárias: O gerenciamento de dados pessoais é a capacidade de identificar registros de dados de titulares em todas as fontes identificadas, fazer sua correspondência e vincular os registros a cada titular de dados individual, bem como criar um repositório do Entity 360. Esse repositório fornece uma fonte de dados de alta qualidade que informa quais registros de dados reais são mantidos nas fontes no escopo e como cada dado é vinculado a um titular de dados individual. O Entity 360 poderia atuar como a fonte autorizada de dados quando as organizações respondem a solicitações de acesso, direito de apagamento ou direito de solicitações de portabilidade do titular. De uma perspectiva de negócios, o Entity 360 pode apoiar as organizações no gerenciamento do consentimento para uso de dados pessoais e, em seguida, no gerenciamento desse consentimento: quando ele é concedido/retirado, por meio de qual canal e quais termos específicos foram acordados?

Caso de uso de tecnologia: O gerenciamento de dados pessoais poderia ser caracterizado como sendo um caso de uso de correspondência e vinculação de dados. Estas são as principais capacidades para identificar registros de titulares dos dados entre sistemas e fornecer uma visão dos dados de todos os sistemas pela correspondência de registros semelhantes e criação de vínculos. As capacidades típicas que poderiam ser aplicadas a esse caso de uso incluem:

- **Acesso a dados relevantes:** Criar um perfil dos dados dos titulares dos dados, extrair dados relevantes de sistemas de origem, aplicar processos analíticos ao conteúdo semiestrutura e não estruturado
- **Processamento de qualidade de dados:** Avaliar os níveis de qualidade de dados, aplicar correção manual/automática, controle de processo para correção manual, relatórios de métricas
- **Única fonte confiável de dados sobre os titulares dos dados, incluindo o consentimento, como ele é obtido e gerenciado:** Inclui diferentes visões e perspectivas sobre o titular, dependendo de seus consentimentos
- **Correspondência e vinculação:** Definir regras de correspondência com base em definições de processo de negócios, fazer a correspondência de registros, vincular registros semelhantes com pontuação, associar o consentimento
- **Persistência de dados:** Persistir registros vinculados/não vinculados, análises e relatórios

Soluções de tecnologia: Adotar soluções que ajudam a descobrir registros de titulares dos dados de todos os domínios de dados, usando algoritmos avançados para fazer a correspondência de todos os dados relacionados ao mesmo titular dos dados, independentemente do local de armazenamento dos dados. O **Informatica Relate 360** utiliza algoritmos avançados para identificar dados associados ao mesmo titular dos dados, e o gerenciamento de dados mestres fornece o quadro para manter e gerenciar uma visão comum de dados sobre os titulares dos dados.

Benefícios: Uma visão única dos indivíduos demonstrou trazer benefícios para os negócios além da GDPR. Isto é especialmente verdadeiro se o indivíduo em questão é um cliente, que cada vez mais espera experiências pessoais adaptadas. De um ponto de vista da GDPR, a capacidade de vincular todos os dados de cada titular dos dados individuais aliviará o fardo de habilitar os direitos do indivíduo. Isso inclui o direito de compreender o uso de dados, o direito de ser esquecido e garantir que o consentimento seja corretamente aplicado.

3.4 Pergunta de ponto de entrada: Como proteger dados e impedir o acesso não autorizado?
Contexto: Os controles de proteção de dados são uma abordagem para interpretar os requisitos de consentimento da GDPR e ajudar a proteger dados pessoais. Poderia haver um requisito da TI para remover, mascarar ou anonimizar os dados de produção utilizados para fins de teste ou para anonimizar dados utilizados para transferências de dados externos. O controle de acesso a dados para os dados pessoais em um nível do usuário em aplicativos deveria ser analisado para fins de conformidade.

Capacidades necessárias: A **detecção e proteção** também oferece controles de acesso e proteção a informações sobre os titulares dos dados. Com frequência, as informações de titulares dos dados são expostas a muitos indivíduos diferentes em uma organização e seu ecossistema. Os controles de segurança de dados são usados para remover ou ocultar as informações de titulares dos dados de quem não deveria ter visibilidade delas, enquanto as informações são disponibilizadas para aqueles que deveriam ter visibilidade.

Caso de uso de tecnologia: A permissão do controle de consentimento poderia ser caracterizada como sendo um caso de uso de detecção e proteção. Estas são as principais capacidades para proteger o acesso a dados, aplicando controles centrados nos dados, como máscara, criptografia e controles de acesso, e para gerenciar o ciclo de vida dos dados, incluindo arquivamento e exclusão de dados e a aplicação. As capacidades típicas que poderiam ser aplicadas a esse caso de uso incluem:

- **Entrada de análise de risco:** Usar a pontuação de risco para direcionar os métodos de controle de dados
- **Orquestração:** A capacidade de agendar e coordenar as tarefas de proteção de dados com base nos riscos identificados e no monitoramento de acesso ou condições não seguras
- **Controles de segurança de dados:** Máscara estática ou dinâmica, acesso baseado em função anonimizado, criptografia ou tokenização.
- **Histórico de alterações/atualizações:** Aplicativo em relação aos sistemas de origem, máscara de registro ou resultados de arquivamento em relação ao registro de consentimento, geração de trilha de auditoria para obtenção de provas
- **Arquivamento:** Arquivar dados fora dos sistemas de produção, registrar em log as atividades para fornecer provas, mover os dados para locais off-line para prevenir o uso ou acesso acidental

Soluções de tecnologia: Adotar soluções que podem ajudar a gerenciar o ciclo de vida de ativos de dados e aplicar controles sobre esses ativos. O **Informatica Persistent Data Masking** e o **Informatica Dynamic Data Masking** poderiam ser usados para ajudar a limitar automaticamente o número de pessoas e de sistemas que têm acesso irrestrito a dados pessoais. O **Informatica Secure@Source** fornece correções de segurança de dados com a orquestração das atualizações de controles de segurança.

Benefícios: Introduzir a automação na máscara de dados a fim de reduzir o risco de violações de dados pessoais. A visibilidade dos dados pessoais é restrita às pessoas autorizadas a visualizá-los, e os dados pessoais não são proliferados sem proteção adequada.

4. Parceiros

Assim como ocorre com muitas formas de regulamentação e conformidade, a tecnologia por si só não garantirá a conformidade. As organizações podem precisar da melhor liderança em ideias inovadoras para sua jornada rumo à GDPR, bem como da entrega da solução tradicional de tecnologia e serviço. A Informatica trabalha com muitos parceiros altamente treinados e qualificados para apoiá-lo em sua iniciativa mais ampla rumo à GDPR. Esses parceiros foram especificamente escolhidos devido à sua profunda compreensão do gerenciamento de dados e ao seu foco na conformidade com GDPR.

Encontre o parceiro certo para você ou entre em contato com seu representante local da Informatica, que poderá ajudá-lo a encontrar o melhor parceiro de acordo com suas necessidades e seus requisitos.

5. Conclusão

Este documento estabelece a necessidade de as organizações considerarem as implicações de dados da GDPR. Esta nova regulamentação traz desafios e oportunidades para muitas organizações. Considerando o curto período até que esta regulamentação entre em vigor, muitas organizações precisarão considerar como sua interpretação dos princípios da GDPR afetará os atuais e futuros processos de gerenciamento de dados.

Para ajudar as organizações a começar rapidamente a operacionalizar essas interpretações, a Informatica delineou algumas das perguntas fundamentais de ponto de entrada que as partes interessadas estão fazendo e sugeriu algumas capacidades que serão necessárias para ajudar a responder a essas perguntas. Essas perguntas e capacidades não apenas abordam uma parte do conjunto de requisitos da GDPR, mas também ajudam a construir todo um conjunto de capacidades para enfrentar muitos dos desafios de dados gerados pela GDPR.

Alinhado a cada capacidade encontra-se um caso de uso de tecnologia. Cada caso de uso descreve os tipos de soluções de software e tecnologias que poderiam ser empregadas para fornecê-lo.

Há mais de 20 anos, a Informatica é o fornecedor líder de gerenciamento de dados, resolvendo desafios complexos de gerenciamento de dados para milhares de organizações no mundo todo. A GDPR criará muitos desafios complexos de gerenciamento de dados para muitas organizações. A Informatica e seu ecossistema de parceiros associados estão perfeitamente posicionados para ajudar essas organizações com suas iniciativas de GDPR.

6. Aviso legal

A conformidade com GDPR será baseada em fatos específicos do uso de dados, operações e negócios de uma organização. Este documento fornece um conjunto de pontos de discussão que podem ser úteis no desenvolvimento de esforços em direção à conformidade com GDPR de uma organização e não se destina a fins de recomendação, orientação ou consultoria jurídica. Uma organização deve consultar seu próprio departamento jurídico sobre quais obrigações devem ou não ser cumpridas.

Informatica

Sede mundial, 2100 Seaport Blvd., Redwood City, CA 94063, EUA Telefone: 650.385.5000 Ligação gratuita nos EUA: 1.800.653.3871 IN09_0218_03337
www.informatica.com/br www.informatica.com linkedin.com/company/Informatica twitter.com/Informatica