Foto de Pedro Lastra on Unsplash

GDPR

101 Controles Básicos para Conformidade

Prof. Ms. Edison Fontes, CISM, CISA, CRISC

Cento e um controles básicos para avaliar conformidade da organização com o Regulamento (UL) 2016/679 do Parlamento Europeu e Conselho.

(GDPR – General Data Protection Regulation)

DOC ELGF.0103.01.0

São Paulo, junho, 2018 - Brasil

Licença para uso deste documento

Este documento

Este documento tem por objetivo indicar cento e um controles básicos que afetam a organização que deve avaliar a sua necessidade de conformidade *(compliance)* com o Regulamento Europeu de Tratamento de Dados (GDPR, Regulamento 2016/679 do Parlamento Europeu e Conselho.

Este documento expõe a opinião e interpretação pessoal do autor, considerando as informações disponíveis neste momento.

Este documento permite uma avaliação inicial para a conformidade da organização em relação aos controles do GDPR. De uma maneira simples, rápida e utilizando poucos recursos, os gestores executivos da organização podem conhecer a situação da organização neste assunto.

Para a implementação da conformidade com o GDPR a organização deve realizar uma avaliação mais detalhada.

Técnica e muito cuidado foram utilizados na elaboração deste documento. Porém erros podem acontecer, tipo digitação ou reprodução. Qualquer erro encontrado, qualquer dúvida de interpretação, solicitamos que seja enviada uma mensagem para edison@pobox.com para a devida verificação e resposta. O autor não assume qualquer responsabilidade por eventuais danos ou perdas a pessoas, organizações ou bens originados do uso deste documento.

O Autor

Edison Fontes é Mestre em Tecnologia, certificado internacional CISA, CISM, CRISC e profissional de segurança da informação. É professor de MBAs, autor de livros e desenvolve atividades de Estrategista, Gestor, Consultor em Segurança Informação, Continuidade de Negócio, Risco Operacional, Conformidade *(Compliance)* da Informação e Combate à Fraude de Informação.

É sócio consultor da Núcleo Consultoria em Segurança

Contato: edison@pobox.com, ef@nucleoconsult.com.br

Livros do Autor

- Segurança da informação: Orientações práticas, Publicação Amazon.
- Políticas de Segurança, Curso RNP, Ministério Ciência e Tecnologia.
- Políticas e Normas para a Segurança da Informação, Editora Brasport.
- Praticando a segurança da informação, Editora Brasport.
- Clicando com segurança, Editora Brasport.
- Segurança da informação: o usuário faz a diferença, Editora Saraiva.
- Vivendo a segurança da informação, Editora Sicurezza.

Documentos do Autor

- Políticas de Segurança da Informação: uma contribuição para o estabelecimento de um padrão mínimo, Dissertação de Mestrado, Centro Paula Souza, Governo Estado de São Paulo.

- GDPR – General Data Protection Regulation – Considerações Edison Fontes. DOC ELGF.0101.02.0

- Política Segurança Cibernética – Computação em Nuvem – Resolução Banco Central do Brasil 4658:2018 – Considerações Edison Fontes. DOC ELGF.0102.01.0

O Regulamento Geral de Proteção de Dados começou a valer a partir de 25 de maio de 2018. É um marco no tratamento da informação de dados pessoais de pessoas singulares e impactará em curto prazo, todas as organizações que utilizam a tecnologia da informação, inclusive as brasileiras que estão no ambiente econômico global.

Photo by Jiyeon Park on Unsplash

INTRODUÇÃO

Baseado no Regulamento Europeu de Tratamento de Dados (GDPR, Regulamento 2016/679 do Parlamento Europeu e Conselho), consolidei 101 Controles Básicos que afetam diretamente a organização. Este conjunto de controles básicos permitem uma avaliação inicial da conformidade da organização em relação ao GDPR.

Alguns controles descritos abaixo, fazem a consolidação de mais de um controle ou a consolidação de um conceito. Eles não são uma pura transcrição das regras do regulamento.

Também chamo atenção para o fato de que um simples controle pode exigir um grande projeto de implantação de medidas, processos e procedimentos de proteção de dados pessoais de pessoas singulares.

Os controles relacionados ao funcionamento da Comissão de Proteção de Dados e dos órgãos de controle dos Estados Membros, não foram contemplados pois não geram obrigações para a organização.

No mês de maio disponibilizei o Documento - GDPR – General Data Protection Regulation – Considerações iniciais, Edison Fontes, DOC ELGF.0101.02.0. Recomendo sua leitura prévia.

1. Necessidade de Aplicação do GDPR – Sim ou Não

Estes sete controles iniciais verificam a necessidade de a organização seguir o GDPR. Caso algum destas perguntas iniciais obter a resposta sim, a organização deve seguir o GDPR pois provavelmente está sujeita a jurisdição prescrita pelo regulamento, devendo garantir a conformidade (compliance) com os controles exigidos no mesmo.

Responda com Sim ou Não. A organização:

1. Coleta ou processa dados pessoais de pessoas de pessoas singulares localizadas na União Europeia? Estas pessoas podem estar visitando o país da sua organização fora da União Europeia.

2. Recebe por transferência dados pessoais de pessoas de pessoas singulares localizadas na União Europeia?

3. Possui matriz, filial ou representação física na União Europeia?

4. Não possui representação física na União Europeia, mas oferece serviços ao mercado da União Europeia? Inclui serviços pela Internet.

5. Monitora dados de pessoas singulares localizadas na União Europeia?

6. Executa serviços de terceirização de processamento de dados para empresas localizadas na União Europeia?

7. É empresa subcontratada de outra empresa que executa serviços de terceirização de processamento de dados para empresas localizadas na União Europeia?

2. Tratamento dos dados pessoais

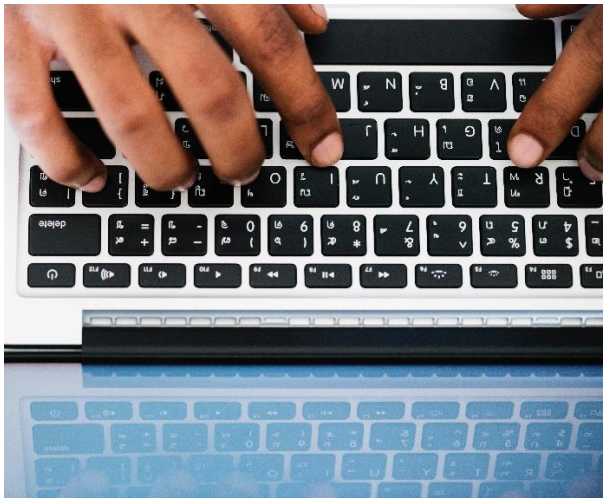


Photo by rawpixel on Unsplash

A organização precisa garantir e ter evidência de que executa os controles abaixo. A organização possui estes controles? Avalie e responda Sim ou Não?

Os controles abaixo estão baseados no regulamento e refletem em interpretação livre do autor que juntou ou separou controles, com o objetivo de facilitar o conhecimento do leitor.

Os controles relacionados ao funcionamento da Comissão de Proteção de Dados e dos órgãos de controle dos Estados Membros, não foram contemplados pois não geram obrigações para a organização.

Solicitação e utilização dos dados

Photo by Gary Bendig on Unsplash

1. Solicitar a autorização explicita da pessoa singular para o tratamento dos dados pessoais.

2. Utilizar os dados exclusivamente para as finalidades determinadas.

3. Utilizar os dados para finalidades legítimas.

4. Não utilizar os dados posteriormente, para outras finalidades. Diferente das finalidades para os quais os dados foram originalmente coletados.

5. Manter os dados exatos e atualizados.

6. Adotar todas as medidas adequadas para que dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora. Garantir a exatidão dos dados.

7. Conservar os dados de forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.

8. Conservar os dados pessoais durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com as leis existentes sobre este assunto.

9. Tratar os dados pessoais de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

10. Tratar dados pessoais para a execução de um contrato no qual o titular dos dados é parte.

11. Conhecer qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior.

12. Garantir que os casos em que o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados, são considerados na legislação.

13. Garantir que se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente

desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples.

14. Garantir e ter mecanismos de tecnologia ou convencionais para que o titular dos dados tenha o direito de retirar o seu consentimento a qualquer momento.

15. Garantir que antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.

16. Guardar evidências do consentimento do titular dos dados.

Coleta de dados de crianças

Photo by Kelly Sikkema on Unsplash

17. Respeitar que a coleta de dados pessoais de crianças é realizada, considerando todas as demais exigências, somente será realizada se elas tiverem pelo menos 16 anos.

18. Garantir que caso a criança tenha menos de 16 anos, o tratamento só acontecerá na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.

Dados pessoais – Origem e opinião da pessoa

Photo by Andrew Neel on Unsplash

19. Não tratar dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

20. Tratar dados pessoais tipo item anterior, exclusivamente para as situações previstas na legislação.

Titular dados pessoais – Informações, direitos, comunicação, apagamento

21. Considerar que nas situações em que não está em condições de identificar o titular dos dados, informar este fato quando do tratamento.

22. Fornecer ao titular as informações, quando necessário, comunicação de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara

e simples, em especial quando as informações são dirigidas especificamente a crianças.

23. Atender ao titular de dados, caso este solicite, a comunicação prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

24. Não recusar a dar seguimento ao pedido do titular no sentido de exercer os seus direitos, exceto se demonstrar que não está em condições de identificar o titular dos dados.

25. Fornecer ao titular dos dados as informações sobre as medidas tomadas, mediante pedido deste titular, sem demora injustificada e no prazo de um mês a contar da data de recepção do pedido.

26. Estender para até dois meses, as solicitações de informação do titular dos dados, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos.

27. Informar ao titular dos dados, quando do recolhimento dos dados diretamente com este titular, as seguintes informações: a identidade e os contatos do responsável pelo tratamento, os contatos do encarregado da proteção de dados e as finalidades do tratamento a que os dados pessoais se destinam, e o fundamento jurídico para o tratamento.

28. Garantir que quando não fornecer as informações citados no item anterior, a situação se encontra nas exceções descritas na legislação.

29. Comunicar ao titular dos dados: o prazo de conservação dos dados pessoais, a existência do direito de solicitar a sua retificação ou o seu apagamento, o direito de apresentar reclamação a uma autoridade de controle.

30. Comunicar ao titular dos dados e obter a sua autorização quando o for proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos,

31. Garantir que o titular dos dados tem o direito de obter a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento.

32. Garantir que o titular dos dados possa saber:

a. As finalidades do tratamento dos dados;

b. Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados,

c. O prazo previsto de conservação dos dados pessoais.

d. A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais.

e. O direito de apresentar reclamação a uma autoridade de controle;

f. Informações sobre a origem desses dados;

g. A definição de perfis e as consequências previstas de tal tratamento.

33. Informar ao titular de dados a transferência dos dados pessoais para um país terceiro ou uma organização internacional, e referidas garantias

34. Possibilitar que o titular dos dados receba uma cópia dos dados pessoais em fase de tratamento.

35. Garantir sem demora injustificada, o conhecimento pelo titular dos dados, a retificação dos dados pessoais inexatos ou incompletos.

36. Garantir o direito do titular dos dados o tratamento de apagamento dos seus dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

a. Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

b. O titular retira o seu consentimento;

c. Os dados pessoais foram tratados ilicitamente;

d. Em função de uma ordem judicial.

37. Informar que o titular dos dados lhes solicitou o apagamento dos dados pessoais aos responsáveis dos diversos ambientes técnicos, quando tiver tornado públicos os dados pessoais e for obrigado a apagá-los, tomando medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação.

38. Comunicar a cada destinatário a quem os dados pessoais tenham sido transmitidos, qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado.

39. Informar ao titular dos dados, quando solicitado, os destinatários (outras organizações, órgãos do governo, filiais, similar) que receberão a comunicação sobre alteração dos dados pessoais.

40. Fornecer ao titular dos dados, os dados pessoais que lhe digam respeito em um formato estruturado de uso corrente e de leitura automática.

41. Garantir que o titular dos dados tem o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados foram fornecidos o possa impedir.

42. Garantir que o titular de dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para efeitos de comercialização direta, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.

Tratamento de dados – Fins científicos, históricos, similar

Photo by chuttersnap on Unsplash

43. Garantir que quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.

44. Avaliar e definir se os dados tratados pela organização são para fins de investigação científica ou histórica e tratar de acordo com a legislação da União Europeia para tal situação.

Nível de confidencialidade

45. Manter os dados pessoais em nível de sigilo confidencial.

Implementação de medidas técnicas

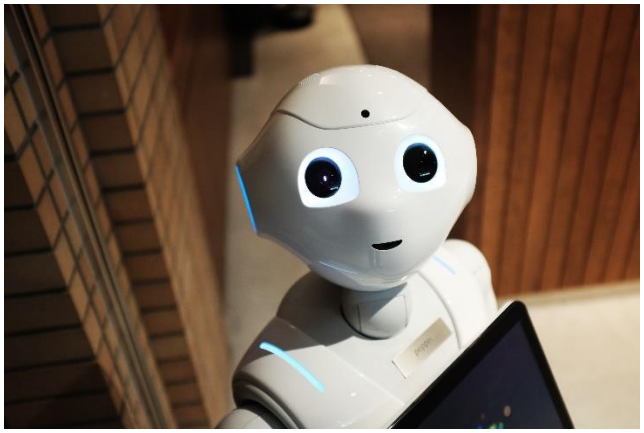


Photo by Alex Knight on Unsplash

46. Garantir que aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o GDPR.

47. Utilizar, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento.

48. Ter medidas que asseguram que, por defeito, os dados pessoais não sejam disponibilizados.

49. Aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, considerando as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares.

50. Utilizar pseudonimização e a cifragem dos dados pessoais;

Tratamento em comum

51. Garantir a existência de acordo, que quando do tratamento em comum com outro, ou mais, responsáveis pelo tratamento de dados, determinem conjuntamente as finalidades e os meios desse tratamento, explicitando que ambos são responsáveis conjuntos pelo tratamento.

Subcontratação para tratamento de dados

Photo by rawpixel on Unsplash

52. Garantir que que quando subcontratar tratamento de dados, recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do GDPR.

53. Garantir que o subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral.

Representante perante autoridades

54. Ter um representante perante as autoridades da União Europeia, caso a organização não esteja estabelecida na União Europeia.

Pessoas autorizadas - Responsabilidades

55. Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade.

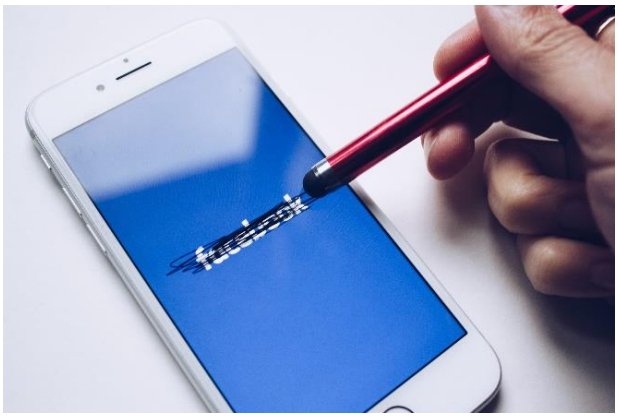


Photo by Thought Catalog on Unsplash

Registro de atividades *(log)*

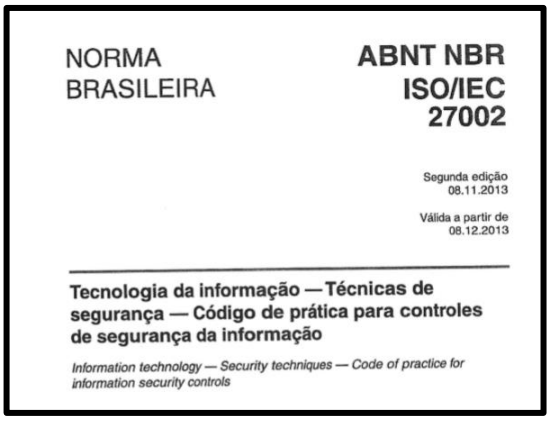
Photo by Brandi Redd on Unsplash

56. Garantir que cada responsável pelo tratamento de dados mantem um registo de todas as atividades de tratamento sob a sua responsabilidade.

Continuidade e Disponibilidade de acesso

57. Ter capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais em tempo adequado e aceitável pelas boas práticas no caso de um incidente físico ou técnico;

Gestão da segurança dos dados


NORMA BRASILEIRA

ABNT NBR ISO/IEC 27002

Segunda edição 08.11.2013

Válida a partir de 08.12.2013

Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação

Information technology — Security techniques — Code of practice for information security controls

Norma NBR 27002:2013

58. Ter um processo para testar, examinar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento de dados pessoais.

59. Ter capacidade para assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento.

60. Avaliar o nível de segurança adequado, considerando os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, armazenados ou sujeitos a qualquer outro tipo de tratamento.

Violação dos dados - Comunicação

61. Comunicar à autoridade de controle qualquer violação de dados pessoais em até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

62. Comunicar ao titular dos dados sem demora injustificável, qualquer violação dos dados pessoais que implicar em um elevado risco para os direitos e liberdades das pessoas singulares.

Avaliação de Impacto – Gestão

Photo by AJ Yorio on Unsplash

63. Realizar sistematicamente avaliação de impacto das operações de tratamento de proteção de dados pessoais. Avaliar o risco para os direitos e liberdades das pessoas singulares.

64. Consultar a autoridade de controle antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.

Encarregado da Proteção de Dados

Photo by Hammad A. on Unsplash

65. Ter um encarregado da proteção de dados com qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções.

66. Envolver o encarregado de proteção de dados de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais.

67. Disponibilizar recursos necessários para o encarregado de proteção de dados desempenhe adequadamente suas funções, mantenha o conhecimento e tenha acesso às operações de tratamento de dados.

68. Garantir que o encarregado de proteção de dados informa diretamente à direção da organização, não recebe instruções relativas ao exercício das suas funções e não pode ser destituído nem penalizado pelo fato de exercer suas funções.

69. Garantir que os titulares dos dados podem contatar o encarregado da proteção de dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais.

70. Garantir que o encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade a legislação da União Europeia.

71. Garantir a não existência de conflito de interesse (segregação de função) do encarregado da proteção de dados, quando o mesmo exercer outras funções e atribuições.

72. Garantir que o encarregado de proteção de dados no desempenho das suas funções, tem em devida consideração aos riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

73. Garantir que quando da existência de certificação de proteção de dados pessoais, a organização buscará esta certificação. A certificação ajudará a explicitar que a organização está em conformidade com a legislação.

Código de Conduta

74. Considerar no código de conduta da organização ou em código de conduta específico, regras para a correta aplicação do GDPR, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas.

75. Exercer supervisão contínua para garantir o cumprimento das disposições do código de conduta na organização e nos parceiros que tratam dados pessoais.

Transferência de dados

Photo by Steve Halama on Unsplash

76. Garantir que qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, as exigências do GDPR forem respeitadas pelo responsável pelo tratamento e pelo subcontratante.

77. Assegurar que, quando de transferência de dados pessoais, não é comprometido o nível de proteção das pessoas singulares garantido pelo GDPR.

78. Garantir que só é realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão Europeia de Tratamento de Dados Pessoais tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado.

79. Garantir que no caso de países ou organizações não autorizadas pela Comissão Europeia, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

Organização e Grupo de Empresas

80. Analisar se a organização pertence a um grupo de empresas envolvidas em uma atividade econômica conjunta e juridicamente vinculativas, para decidir a melhor implementação do controle de proteção dos dados pessoais.

Photo by Sven Read on Unsplash

Autoridades administrativa de país terceiros ou Estados Membros

81. Garantir que, quando aplicáveis à organização, as decisões judiciais e as decisões de autoridades administrativas de um país terceiro que exijam que o responsável pelo tratamento ou o subcontratante transfiram ou divulguem dados pessoais só serão executadas se tiverem como base um acordo internacional.

82. Garantir que a organização está ciente da autoridade ou das diversas autoridades públicas independentes dos Estados Membros da União Europeia que exercem a fiscalização da aplicação do GDPR.

Comitê União Europeia de Proteção de Dados

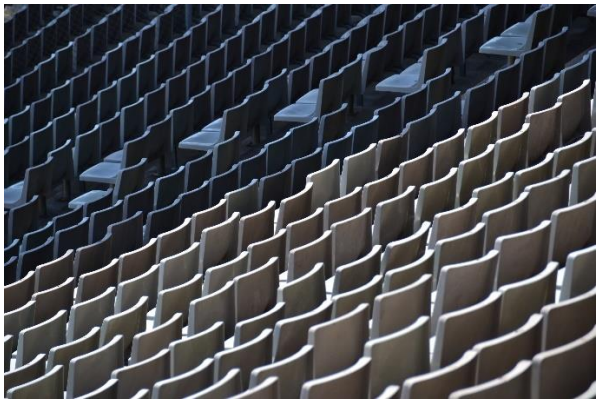


Photo by Andrea Junqueira on Unsplash

83. Acompanhar e aprender como o relatório anual de atividades, que o Comitê de Controle do Estado Membro divulga, contendo uma lista dos tipos de violação notificadas e dos tipos de medidas tomadas.

84. Acompanhar e aprender como o relatório anual de atividades, que o Comitê Europeu para a Proteção de Dados que divulga um relatório anual sobre a proteção das pessoas singulares no que diz respeito ao tratamento na União e, quando for relevante, em países terceiros e organizações internacionais.

85. Cooperar quando solicitado com as autoridades de controle e com a Comissão Europeia de Proteção de Dados Pessoais.

Mapeamento dos Dados Pessoais

Photo by Valentino Funghi on Unsplash

86. Garantir que a organização tem mapeado o fluxo de existência dos dados pessoais.

87. Garantir que a organização tem uma estruturação técnica de maneira a facilitar a proteção e a rastreabilidade dos dados pessoais.

Direito de reclamação à autoridade de controle

Photo by Benjamin Ashton on Unsplash

88. Estar ciente de que a organização, como titular de dados, tem direito a apresentar reclamação a uma autoridade de controlo, em especial no Estado-Membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada a infração.

Sigilo

Photo by Daniel von Appen on Unsplash

89. Garantir que a organização segue normas específicas instituídas pelos organismos nacionais competentes, a uma obrigação de sigilo profissional ou a outras obrigações de sigilo equivalentes.

Igreja e comunidade religiosa

Photo by Mathilde Cureau on Unsplash

90. Analisar se a organização é uma igreja ou comunidade religiosa e seguir a legislação em vigor no seu detalhe para este tipo de organização, sabendo que está sujeita a uma autoridade de controle independente.

Direitos específicos

Photo by rawpixel on Unsplash

91. Estar ciente que os Estados Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral.

Avaliação e revisão do GDPR

Photo by Firdouss Ross on Unsplash

92. Acompanhar os relatórios que a Comissão de Proteção de Dados apresenta ao Parlamento Europeu avaliando ou revisando o GDPR.

93. Acompanhar a Comissão de Proteção de Dados que apresenta propostas legislativas com vista à alteração de outros atos jurídicos da União sobre a proteção dos dados pessoais. Manter a conformidade com as novas regras.

Penalidades

94. Considerar e conscientizar o Corpo Diretivo que a organização, caso não cumpra as regras do GDPR, pode sofrer multas que podem chegar a vinte milhões de euros ou até 4% do faturamento bruto do ano anterior.

Photo by pina messina on Unsplash

Photo by Carles Rabada on Unsplash

CONCLUSÃO

Analise as suas respostas e identifique qual a maturidade dos controles existentes para o atendimento ao Regulamento da União Europeia para a Proteção de Dados de Pessoas Singulares.

Neste momento as organizações estão caminhando para aprimorar os seus controles de segurança da informação para suportar os controles específicos do GDPR. Ter um Processo Corporativo de Segurança da Informação é um elemento estrutural para o atendimento ao GDPR. Na figura abaixo apresentamos controles do GDPR que devem ser suportados por controles de segurança da informação.

		DIMENSÕES E CONTROLES DE SEGURANÇA DA INFORMAÇÃO															
GDPR - RESOLUÇÃO DE PROTEÇÃO DE DADOS PESSOAIS (EU) Edison Fontes, 2018 ⬇	Macrocontroles	Política de S.I.	Acesso/uso Informação	Classificação Informação	Proteção Técnica	Flexibilidade Operacional (Inc. Prob. Mud.)	Desenvolv. Aplicativos (Seguro)	Continuidade Negócio	Cópias de Segurança	Gestão de Ricos Informação	Treinamento e Conscientização	Ambiente Físico	Modelo Operativo S.I.	Criptografia	Gestão capacidade TIx Negócio	Prestadores Serviço e Fornecedores	Processo Organizacional S.I.
Art. 1 - Objeto	Tratamento dados pessoais		X	X													
Art. 3 - Ambito	Ambito aplicação territorial															X	
Art. 5 - Tratamento	Integridade, finalidade uso, segurança	X	X		X			X									X
Art. 6 - Licitude do tratamento	Validade para tratar a informação		X														
Art. 7 - Consentimento	Condições aplicáveis de consentimento		X														
Art. 9 - Categorias especiais	Tratamento de categorias especiais			X													
Art. 12 - Transparencia	Comunicação das regras										X						
Art. 13 - Recolhimento Titular	Autorização uso, cópias, retenção, diretriz		X						X								
Art. 14 - Recolhimento não Titular	Autorização uso, cópias, retenção, diretriz		X						X								
Art. 15 - Direito acesso	Retenção, copia, apagamento		X						X								
Art. 16 - Direito Retificação	Correção, apagamento		X														
Art. 17 - Direito Apagamento	Apagamento		X					X									
Art. 20 - Portabilidade Dados	Recebimento de dados pessoais		X														
Art. 23 - (2b) - Limitações	Tratamento dados pessoais			X													X
Art. 24 - Responsabilidaded	Responsabilidade no tratamento	X			X						X						X
Art. 28 - Subcontratante	Subcontratante															X	
Art. 30 - Registro atividades	Registro atividades tratamento		X													X	X
Art. 32 - Segurança do tratamento	Segurança, continuidade, gestão riscos,				X	X	X	X	X	X	X			X	X		X
Art. 33 - Violação de dados	Notificação à autoridade de controle					X											
Art. 34 - Violação de dados	Notificação ao titular dos dados					X											
Art. 35 - Avaliação impacto	Avaliação impacto proteção dados					X				X							
Art. 36 - Consulta prévia	Consulta prévia risco elevado					X				X							
Art. 37 - Designação encarregado	Encarregado proteção de dados												X				
Art. 38 - Posição do encarregado	Posição na organização												X				
Art. 39 - Funções do encarregado	Funções de responsabilidade do												X				
Controles de Segurança		OK	OK	OK	OK	OK	OK	OK	OK	OK	OK		OK	OK	OK	OK	OK
Frequencia		*2*	*11*	*3*	*3*	*5*	*1*	*3*	*4*	*3*	*3*	*0*	*3*	*1*	*1*	*3*	*5*

Controles GDPR x Controles NBR 27002:2013

Edison Fontes, CISM, CISA, CRISC
Sócio Núcleo Consultoria
Estrategista, Consultor e Gestor: Segurança da Informação, Riscos, Continuidade e Combate à Fraude, Compliance.
Coordenador do Comitê de Segurança da Informação da ABSEG.

edison@pobox.com, ef@nucleoconsult.com.br, www.nucleoconsult.com.br

========== Fim do Documento ==========