Levantamento de iniciativas para a adequação à LGPD na Fiocruz.

A Lei n.º 3709/2018 (Lei Geral de Proteção de Dados /LGPD) dispõe sobre o tratamento de dados pessoais, onde deverão ser cumpridas diversas obrigações legais, além de procedimentos preliminares de segurança e governança e passou a vigorar em setembro de 2020.

Inicialmente, a adequação das instituições à LGPD envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional. Essa transformação tem fundamentos, dentre eles a autodeterminação informativa dos titulares dos dados. A autodeterminação informativa consiste no direito de o titular dos dados pessoais conhecer o processo de tratamento de seus dados em sua integralidade, o porquê, para quê, como, por quem e onde seus dados são tratados. Esta deve ser considerada desde a fase de concepção do serviço, produto ou banco de dados até sua execução. A adequação envolve também promover ações de conscientização de todo corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Visando identificar possíveis iniciativas para a adequação à LGPD nos órgãos/unidades da Fiocruz, e mitigar riscos de não implementação solicitamos ao Coordenadores dos Comitês de Gestão de Integridade, Riscos e Controles Internos da Fiocruz que preencham o questionário abaixo até o dia 04/06/2021.

Em caso de dúvida, por favor enviar e-mail para governancadedados@fiocruz.br

* Obrigatória

1. Órgão/Unidade da Fiocruz *

2. Você conhece a LGPD, sabe do que se trata? *

- ◯ Sim
- ◯ Não

3. Nome do servidor responsável pelas respostas ao questionário *

4. E-mail do servidor responsável pelas respostas ao questionário *

5. O órgão/Unidade planejou alguma medida necessária para a adequação à LGPD? *

- ◯ Sim
- ◯ Não

6. Se sim planejou, qual foi? (grupos de trabalho, levantamento de outros normativos que devem ser respeitados sobre informações pessoais, políticas de segurança e/ou privacidade, termos de consentimento, plano de ação, relatórios, recursos criptográficos, outras medidas de tratamento e segurança para informação pessoal, entre outras) *

7. O órgão/Unidade executou alguma medida necessária para a adequação à LGPD? *

- ◯ Sim
- ◯ Não

8. Se sim, executou qual foi? (grupos de trabalho, levantamento de outros normativos que devem ser respeitados sobre informações pessoais, políticas de segurança e/ou privacidade, termos de consentimento, plano de ação, relatórios, recursos criptográficos, outras medidas de tratamento e segurança para informação pessoal, entre outras) *

9. O órgão/unidade promoveu iniciativas para conscientizar e capacitar os colaboradores em proteção de dados pessoais? *

- ◯ Sim
- ◯ Não

10. Se sim, quais iniciativas e capacitações realizou? (sobre as capacitações informar data, instituição e carga horária e quantos colaboradores participaram; informar como iniciativas encontros, seminários entre outros) *

11. Seu órgão/unidade faz tratamento de dados pessoais? (tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; dado pessoal: informação relacionada a pessoa natural identificada ou identificável) *

- ◯ Sim

12. Se sim, que tipo de dado pessoal trata?

13. Se sim, com que finalidade? (Para responder a esta pergunta tome como base a quadro da página 23 do Guia de Boas Práticas da LGPD - https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf) *

14. Se sim, em quais processos/serviços/banco de dados institucionais é realizado o tratamento de dados pessoais?

15. Seu órgão/unidade faz tratamento de dados pessoais sensíveis? (dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural) *

- ◯ Sim

16. Se sim, qual dado pessoal sensível? *

- [ ] dados que revelam origem racial ou étnica
- [ ] dados que revelam convicção religiosa
- [ ] dados que revelam opinião política
- [ ] dados que revelam filiação a sindicato
- [ ] dados que revelam filiação a organização de caráter religioso
- [ ] dados que revelam filiação ou crença filosófica
- [ ] dados que revelam filiação ou preferências políticas
- [ ] dados referente à saúde ou à vida sexual
- [ ] dados genéticos
- [ ] dados biométricos

17. Se sim, em quais processos/serviços/banco de dados institucionais é realizado o tratamento de dados pessoais sensíveis?

18. O órgão/unidade possui Politica de privacidade (ou instrumento similar)? *

- ◯ Sim
- ◯ Não

19. Se sim possui, esta publicada da internet? *

- ◯ Sim
- ◯ Não

20. Se sim, esta publicada da internet informe o endereço da internet onde esta publicada (URL)

21. Seu órgão/unidade compartilha dados pessoais com algum outro órgão ou entidade nacional ou internacional? *

- ◯ Sim
- ◯ Não

22. Se sim, quais órgãos/atividades envolvem esse compartilhamento de dados?

23. Você sabe indicar quem são os profissionais/áreas que tratam dados pessoais ou pessoais sensíveis em seu órgão/unidade? *

- ◯ Sim
- ◯ Não

24. Se sim, quais áreas/profissionais? (informar área, nome e e-mail)

25. Quais dos riscos abaixo que geram impacto potencial sobre o titular de dados pessoais você identifica no seu órgão/unidade? (em caso de dúvidas conceituais consultar paginas 12 a 14 do Guia de Avaliação de Riscos de Segurança e Privacidade - https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-avaliacao-de-riscos-de-seguranca-e-privacidade.pdf) *

- [ ] Acesso não autorizado - Acesso indevido (permissões indevidas) a um ambiente físico ou lógico
- [ ] Modificação não autorizada - Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada.
- [ ] Perda - Perdas provocadas por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, e provenientes de ações não intencionais como falhas em sistemas, sobrescrita de dados, falhas em hardware, entre outras.
- [ ] Roubo - Dados roubados nas dependências interna do controlador/operador, falhas nos controles de segurança dos sistemas (a exemplo da ausência ou fraca criptografia, falha de sistema que permita escalação de privilégio ou tratamentos indevidos), entre outras.
- [ ] Remoção não autorizada - Usuário não tem a permissão para retirar ou copiar dados pessoais para outro local.
- [ ] Coleção excessiva - Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.
- [ ] Informação insuficiente sobre a finalidade do tratamento
- [ ] Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente)
- [ ] Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)
- [ ] Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais
- [ ] Retenção prolongada de dados pessoais sem necessidade.
- [ ] Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.
- [ ] Falha ou erro de processamento (Ex.: execução de script de banco de dados que

26. Se sim, quais ações/controles foram planejadas? *

27. Se sim, quais ações/controles foram implementadas? *