

ルクセンブルク データ保護国家委員会 (CNPD)

新しいデータ保護のルールに対する準備は出来ていますか？

一般データ保護規則 (GDPR) への準備に役立つ 10 の質問

www.cnpd.lu で随時更新しています。

1995 年の EU 一般データ保護指令及び 2002 年のルクセンブルク法は廃止され、一般データ保護規則に基づく一元的な欧州データ保護体制が成立します。

新しい、強化された個人の権利をご存知ですか？

既存の権利 (例：アクセス権、修正権) に加えて、データ管理者は、消去権 (「忘れられる権利」) 及びデータ・ポータビリティの権利等、データ主体にとっての新しい、拡張した権利に対し準備する必要があります。あなたの組織には、個人データを個人又は他の組織に電子的かつ「構造化された機械可読」のある形式で移転する手続がありますか？

2018 年 5 月 25 日までに GDPR を遵守しなければならないことをご存じですか？

同日 (2018 年 5 月 25 日) まで現行のデータ保護に係る国内法が適用されますが、今の段階から、新しい法的枠組があなたの組織に及ぼす影響を予測しておく必要があります。十分な時間と資源を配分し、その日までに GDPR を確実に遵守できるようにしておくことが重要です。

あなたの組織は何らかの影響を受けるのでしょうか？

GDPR は、EU 域内に所在する組織 (データ管理者及びデータ処理者) に適用されるだけでなく、EU 域外の組織のうち、EU 内の個人に物品又はサービスを提供したり、行動を監視したりしているものにも適用されます。つまり GDPR は、従前はデータ保護体制の対象外だった組織にも影響を与えるのです。

個人データ処理活動について知っていますか？

効果的なデータ保護のための第一歩は、全ての個人データ流通 (従業員データ、顧客データ等) について、特定と文書化を行うことです。既存のデータ処理の法的根拠と目的は何ですか？ データの提供元と提供先は誰ですか？ データはどこに保存され、誰がアクセスできますか？ GDPR において、データ管理者とデータ処理者は、処理活動の詳細な記録を保管することとされています。

データ保護に配慮した製品やサービスを開発または利用していますか？

各組織は、デザインアプローチによるデータ保護を行わなくてはなりません。つまり、新しいシステムやサービスの設計、実施、利用時に、プライバシーやセキュリティ対策を考慮する必要があります。プライバシーリスクが高いプロジェクトでは、データ保護影響評価 (DPIA) が必要となります。場合によっては、データを処理する前に CNPD に相談する必要があります。また、組織のデータ処理活動に当たり関係すると思われるプライバシー強化技術について、情報収集しておくこともおすすめです。

データ保護オフィサーを任命する必要があるのでしょうか？

GDPR では、公的機関又は、企業のうち、処理活動において定期的かつ体系的な個人の監視を行うものについて、データ保護オフィサー (DPO) を任命しなければならないとされています。DPO は、個人データの保護に関する全ての事柄に関与しなければなりません。あなたの組織でも、DPO を任命する必要があるかどうかを今すぐ検討する必要があります。あなたの組織内にデータ保護に関する

ことを担当できる人がいますか？ そうでない場合、新しい人材を雇用する必要はないでしょうか？

適切なセキュリティ対策が施されていますか？

GDPR では、必要なセキュリティ対策について定期的に文書化し、再検討する必要があります。データ処理のリスクに対し、適切なセキュリティ・レベルを確保できますか？ 事故（人災）が発生した場合、個人情報情報を復元することはできますか？ 機微データの機密性と完全性をどのように保証しますか？

個人データ漏洩発覚から 72 時間以内に CNPD に報告しなければならないことをご存じですか？

データ違反がデータ主体の権利と自由にリスクをもたらす可能性が高い場合にのみ、この義務が課されます。このリスクが高い場合、データ管理者は影響を受けるデータ主体に対し、違反の事実を伝えなければなりません。

データ処理者においては、データの漏えいをデータ管理者に通知する適切な手順を備えているかどうか、確認しておかなければなりません。

規制に違反している組織には今よりも厳しい罰則が課されることをご存じですか？

ルクセンブルクのデータ保護当局である CNPD は、データ管理者に重大な規則違反に責任がある場合、2000 万ユーロ又は当該事業者が事業を展開している全ての国における年間売上高合計の最大 4%のいずれか高額の罰金を課すことができるようになります。

現行のデータ処理契約を再検討して変更する必要がありますか？

データ管理者の代わりにデータ処理者によって行われるデータ処理は、データ処理者・データ管理者間の契約または他の法的行為によって行わなければなりません。GDPR では、契約又はその他の法的行為の内容について、さらに具体的に規定されています。

あなたはデータ管理者ですか？ データ処理者ですか？

データ管理者：個人データの処理の目的と手段を決定します。

データ処理者：データ管理者の代わりに個人データを処理します。

Commission nationale pour la protection des donnees

1, avenue du rock'n'Roll

L-4361 Esch-sur Alzette

Tel: (+352) 26 10 60-1

Fax: (+352) 26 10 60-29

E-mail: info@cnpd.lu