【CNPD　COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES】

ルクセンブルク　データ保護国家委員会

ARE YOU READY FOR THE NEW DATA PROTECTION RULES?

新しいデータ保護規則に対する準備は出来ていますか？

10 questions to help prepare your organization for the General Data Protection Regulation (GDPR).

あなたの組織が一般データ保護規則に備えるのに役立つ 10 の質問。

TO STAY UPDATED, VISIT WWW.CNPD.LU

www.cnpd.lu で随時更新しています。

The General Data Protection Regulation will establish a single European data protection regime, replacing the directive from 1995 and Luxembourg's law from 2002.

一般データ保護規則により、1995 年の指令と 2002 年のルクセンブルクの法律に代わる唯一の欧州データ保護体制が成立します。

Are you aware of the new and strengthened rights of individuals?

新しい強化された個人の権利をご存知ですか？

Besides existing right (e.g. right to access, right to rectification), data controllers will have to prepare for new and extended right of data subjects such as the extended right to erasure ("right to be forgotten") and the right to data portability. Do you have procedures in place to transfer personal data to individuals or to other organizations electronically and in a "structured machine-readable" format?

現行の権利（例えば、アクセス権、修正権）に加えて、データ管理者は、拡大された消去権（「忘れられる権利」）及びデータ可搬性の権利等、データ主体の新しい、拡張した権利について備えなければなりません。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」形式で移転する手続は整備してありますか？

Do you know that you have to comply with the GDPR by May 25th, 2018?

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？

While existing national data protection laws will continue to apply until that date, time has come to assess the impact the new legal framework will have on your organization. It is important to allocate enough time and resources to ensure that compliance with the GDPR is achieved before that deadline.

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、今から、新しい法的枠組があなたの組織に及ぼす影響を評価しておく必要があります。十分な時間と資源を配分し、期限までにGDPR を確実に遵守できるようにすることが重要です。

Is your Organization affected?
あなたの組織は影響を受けるのでしょうか？

The GDPR will not only apply to organizations established in the EU (data controllers and processors), but also to organizations established outside the EU offering goods or services to, or monitor the behavior of, individuals in the EU. This means that the GDPR will also affect organizations previously not subject to the data protection regime.

GDPR は、EU 域内に設立された組織（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 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 EU 域外の組織にも適用されます。これは、GDPR が、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ことを意味します。

Are you aware of your personal data processing activities?
あなたの組織は個人データ処理活動を認識していますか？

A first step towards effective data protection in your organization consists in identifying and documenting all personal data flows (e.g. employee data, customer data). What is the legal ground for any existing data processing and what is its purpose? Where does the data come from and who are the recipients? Where is the data stored and who can access it? The GDPR will require controllers and processors to maintain detailed records of processing activities.

あなたの組織における効果的なデータ保護のためにまずやるべきなのは、全ての個人データ流通（従業員データ、顧客データ等）の特定と文書化です。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 は、データ管理者とデータ処理者が処理活動の詳細な記録を保管することを要求しています。

Are you developing or using data protection friendly products and services?
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？

Organizations have to adopt a Data protection by design approach. This means that they should take into account privacy and security measures when designing, implementing or using new systems and services. Data Protection Impact Assessment (DPIA) will be required for projects where privacy risks are high. In some cases, you will be required to consult the CNPD prior to processing. It is also good practice to keep yourself informed about privacy enhancing technologies that might be relevant in the context of the organization's data processing activities.

組織は、デザインアプローチによるデータ保護を採用し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、使用時に、プライバシーやセキュリティ対策を考慮する必要があるのです。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（DPA）が必要となります。場合によっては、データ処理前に 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関す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。

Will you have to appoint a Data Protection Officer?

データ保護責任者を任命しなければなりませんか？

The GDPR requires that public authorities or companies whose processing activities include the regular and systematic monitoring of individuals appoint a Data Protection Officer (DPO). The DPO has to be involved in all matters that concern the protection of personal data. You should assess now whether you should appoint a DPO. Do you have people within your organization that could be put in charge of data protection issues? If not, do you need to hire somebody?

GDPR は、公的機関又は定期的かつ体系的な個人の監視を含む処理活動を行う企業において、データ保護責任者（DPO）を任命することを要求しています。DPO は、個人データの保護に関わる全ての事項に関与しなければなりません。DPO を指定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の問題を担当できる人がいますか？　そうでない場合は、誰かを雇う必要がありますか？

Do you have appropriate security measures in place?

適切なセキュリティ対策が施されていますか？

The GDPR requires you to regularly document and to review the security measures you have in place. Can you ensure a level of security appropriate to the risks of the data processing? Are you able to restore the personal data in case of an incident? How do you guarantee the confidentiality and integrity of sensitive data?

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、適切なレベルのセキュリティを確保できますか？　インシデント（人災）発生時に個人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？

Do you know that you must report a personal data breach to the CNPD within 72 hours after its detection?

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？

This obligation only holds if the data breach is likely to pose a risk to the right and freedoms of the data subjects. If this risk is high, then the controller also has to communicate the breach to affected data subjects.

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、この義務が発生しま

す。このリスクが高い場合、データ管理者は影響を受けたデータ主体に違反の事実を伝えなければなりません。

If you are a data processor, you should make sure that you have the right procedures in place to inform the controller of data breaches.

データ処理者の場合は、データ取扱事業者にデータ漏えいを知らせるための適切な手順を備えていることを確認する必要があります。

Do you know that there will be tougher penalties for organizations that breach the Regulation?

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？

The CNPD, Luxembourg's data protection authority, will be able to impose fines of 20 million euros or up to 4% of the total worldwide annual turnover (whichever is the greater), where controllers are responsible for serious breaches of the Regulation.

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%のいずれか高額の方の罰金を課すことができるようになります。

Will you have to review and update (if necessary) existing contracts with data processors?

現行のデータ処理契約を再検討して更新する必要はありますか？

Data processing that is carried out by a processor on behalf of a controller has to be governed by a contract or another legal act that binds the processor to the controller. The GDPR further specifies the content of the contract or other legal act.

データ管理者の代わりにデータ処理者によって実行されるデータ処理は、データ処理者とデータ管理者を結び付ける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、契約の内容またはその他の法的行為についてさらに具体的に規定されています。

Are you a data controller or a processor?

あなたはデータ管理者ですか？　データ処理者ですか？

DATA CONTROLLER: determines the purposes and means of the processing of personal data

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

DATA PROCESSOR: processes personal data on behalf of a data controller

データ処理者：データ取扱事業者の代わりに個人データを処理します

Commission nationale pur 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