LuxTrust inaugure sa filiale «LuxTrust France» à Paris

La société de services de confiance LuxTrust a inauguré le 9 janvier sa filiale française en présence d'Etienne Schneider, Vice-Premier ministre, ministre de l'économie et de la santé du Grand-Duché de Luxembourg. LuxTrust confirme ainsi son positionnement international et la stratégie pan-européenne poursuivie avec son partenaire InfoCert.

En présence de ses actionnaires, partenaires, clients et du ministre LuxTrust a inauguré sa filiale française, «LuxTrust France» située sur l'avenue des Champs Elysées au centre de Paris.

La société qui gère l'identité numérique et les services de confiance de tous les citoyens et entreprises du Luxembourg s'étend ainsi au-delà des frontières et amène son expertise au marché français sur des sujets tels que la gestion d'identité numérique, la dématérialisation complète des processus et la signature électronique.

De gauche à droite : Pascal ROGIEST, CEO de LuxTrust, Marco GOELER, SNCI, Etienne SCHNEIDER, Vice-Premier ministre, Serge ALLEGREZZA, président de Luxtrust, Martine SCHOMMER, Ambassade de Luxembourg à Paris, Frédéric TOURRET, LuxTrust © LuxTrust

Un choix stratégique

«Nous établir à Paris est un choix stratégique pour répondre aux besoins de proximité de nos clients et partenaires français de plus en plus nombreux.» se félicite Astrid Clausse, directrice commerciale de «LuxTrust France».

Se développer grâce aux partenaires

«Si au départ le cœur de métier de LuxTrust était axé sur l'identité numérique et les services de confiance, nous avons depuis étendu nos solutions digitales afin de mieux répondre aux challenges des entreprises. Ces solutions adressent notamment les problématiques de gestion documentaire et de signatures multiples, ainsi que de gestion d'informations personnelles. L'application efficace de ces solutions ne peut se faire qu'avec l'aide de partenaires forts et engagés que nous nous réjouissons d'avoir déjà en France.» souligne Pascal Rogiest, CEO de LuxTrust.

Une table ronde sur l'identité numérique a eu lieu à l'occasion de l'inauguration avec Marco Di Luzio, CMO d'InfoCert (Italie), Kris de Ryck, CEO de itsme® (Belgique), Cédric Clément, responsable du pôle numérique de la Caisse de Dépôts et Consignations (France) et Etienne Combet, co-fondateur de SEALWeb. Les discussions ont porté sur l'évolution de l'identité numérique et des services de confiance avec comme objectif l'interopérabilité des systèmes en Europe.

Une société luxembourgeoise devenue européenne

«LuxTrust est aujourd'hui un de ces multiples facteurs qui font du Luxembourg depuis de nombreuses années un lieu privilégié pour le marché digital et les services innovants de confiance numériques. Désormais, ce n'est plus d'une société luxembourgeoise dont on parle, mais d'une société européenne» a déclaré le Vice-Premier ministre Etienne Schneider lors de son allocution.

Avec un actionnariat composé à 50% de la société italienne InfoCert, membre du groupe TINEXTA, des bureaux ouverts à Paris et à Bruxelles, LuxTrust ne cache pas son ambition de confirmer avec InfoCert et Camerfirma leur position de leader européen des services de confiance numérique, tout en assurant une présence et une confiance locale dans les géographies prioritaires, parmi lesquelles la France.

Implement the GDPR - how to get started

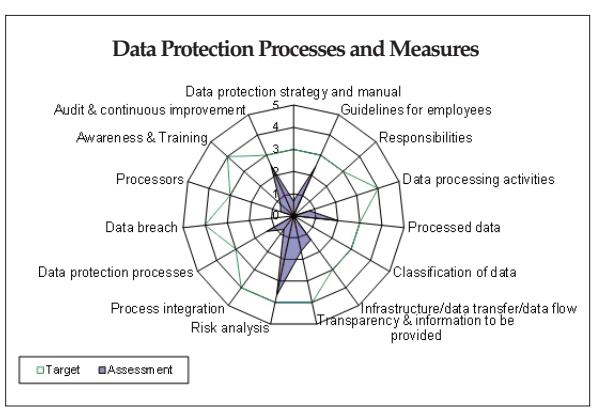
By Lionel GENDARME, Advisory Partner and Shariq ARIF, Advisory Manager, Grant Thornton Luxembourg

Knowing how to implement the requirements of the GDPR may appear unclear, as many firms have not done it to date, and struggle to figure out where to start. Since Grant Thornton has supported a number of firms implement the regulation in multiple sectors, this article describes a series of pragmatic guidelines on implementing the GDPR. This approach is equally relevant in a large multinational and a small SME.

How does it work?

We typically start GDPR implementation by performing an impact analysis. To do so we use a tool that comprises various lists of questions that are designed to assess the firm's business and IT contexts and consider which GDPR requirements apply most to the firm.

The answers to questions put forward enables us to rapidly identify gaps, generating an overall picture on the current state of the firm's organisational and information security measures in place to manage personal data protection. Captions below show snapshots of the gap analysis outcome for a firm that was assessed as having strong information security measures that exceed targets, but lack robust organisational measures.



We then use the results of this impact analysis to define an implementation roadmap. Based on our experience, when implemented, this roadmap should at the minima address the following requirements.

Requirement 1: Be transparent on the personal data that the firm processes

The GDPR requires firms to be transparent on the way they process personal data. Personal data can be as simple as an individual's name, or any other identifier that can be used to spot them. The firm is obliged to inform these individuals accordingly about the rights they have on their personal data, including consultation, correction, and limiting its transfer or deletion. These rights are designed to give back control to individuals on how their personal data is processed. Communication to individuals on processed personal data and related rights is usually made at the time that the firm receives personal data from individuals. For employees this can be conveyed in their employment contract. It is also a common practice to make this communication publically available on the firm's website.

Requirement 2: Keep a register of the processes in place within the firm that involve personal data

The GDPR requires firms to ensure that they collect personal data for a specific purpose. This data should be kept up to date and stored for no longer than permitted based upon a pre-determined commercial purpose or because the law requires it.

To fulfil these duties, we strongly encourage firms to put in place a register of all processes that involve personal data. This register provides a snapshot of all types of personal data processing activities administered by the firm, which often pertain to marketing, provision of services and legal obligations.

This register can effectively be built and maintained using Microsoft Office in simple structures, and can be reinforced with workflows that outline how personal data flows, to better visualise personal data processing activities.

Requirement 3: Sign data protection clauses with the firm's service providers

The GDPR requires firms to keep a solid handle on the personal data it processes and act responsibly at all times, even if it outsources some processes to third parties. This can occur when firms decide to house their personal data in data centres managed by third parties, or appoint specialist external payroll service providers to administer salaries and benefits.

A firm can leverage on the register of personal data processes described above to identify third parties with which it shares personal data, and sign data protection clauses with them. Such clauses must outline how personal data is handled and provide assurance to the firm that third parties have adequate organisational and information security measures in place to guarantee that they process the firm's personal data in compliance with the regulation.

Should the involvement of a third party lead to the firm's personal data being transferred to countries outside of the European Economic Area that do not offer levels of protection considered equivalent by the European Commission, we advocate defining additional contractual measures that provide assurance on the way the third party will process the firm's personal data.

Requirement 4: Establish efficient organisational measures to address a data breach occurring within a firm

It can, and it often happens that personal data is breached. A breach of personal data can be something as simple as sending a mail containing personal data to a recipient who is not supposed to become aware of this personal data. It can also be a case of having an electronic file corrupted that the firm is unable to restore. It may also be a case of having one's identity stolen such as when an employee's inbox is hacked.

Identification of a data breach can be detected by a tool, but more often is notified by individuals. Therefore, the firm needs to raise awareness amongst staff to explain what events can be considered as a personal data breach so that they are rapidly escalated to the person in charge of personal data protection as described below. This person is best placed to assess whether the event constitutes a personal data breach and is worthy of being notified to the CNPD. Irrespective of whether the CNPD or the concerned person is informed, a log of all incidents needs to be kept at the firm. If the event is considered a personal data breach, then in parallel, measures need to be taken to limit any potential risk. We encourage firms to have an action plan in place for decision makers at the firm to know which steps need to be taken to rapidly address the breach.

Requirement 5: Have one person in charge of data protection

Because the implementation of the GDPR is a continuous project, we strongly advocate to have one person in the firm that oversees it is adhered to. This person has several duties that include raising awareness on the regulation via trainings or e-learning sessions, and being a source of advice to the business. Advice can encompass respecting the GDPR when implementing digitalisation projects that often involve the processing of personal data. It can also extend to overseeing the data protection implications in marketing campaigns. In this instance, this person should guide the marketing team on how to ensure promotional content is only shared with clients that have given their consent, and are provided with the ability to unsubscribe at any point in time.

When firms proceed to practice the requirements outlined above, the foundations of the GDPR are set. The impact analysis and the requirements that follow, enable the firm to have a proportionate and practical mechanism in place to achieve GDPR compliance. By following a pragmatic approach, firms inspire confidence to relevant stakeholders that their personal data processes are carried out in a structured and responsible manner.

In a forthcoming publication, we will describe practical steps to effectively manage data breaches.