L'utilisation du smartphone toujours en hausse au Luxembourg

Deloitte Luxembourg vient de publier la version locale de son étude «Global Mobile Consumer Survey 2017». Selon l'enquête, non seulement les Luxembourgeois possèdent plus de smartphones que leurs voisins, mais ils les utilisent également plus souvent, sauf lors des repas ou pour le paiement de factures. En moyenne, le taux d'adoption des smartphones se situe à environ 80 pour cent dans les pays développés.

Au Luxembourg, cette proportion s'élève désormais à 91 pour cent de la population adulte, une hausse de 3 pour cent par rapport à l'année dernière. L'enquête suggère par ailleurs que la population du Grand-Duché a une utilisation très active des téléphones portables. Qui plus est, 54 pour cent des détenteurs de smartphones au Luxembourg ont opté pour la marque Apple, la plus populaire actuellement, ce qui représente une augmentation de 4 pour cent par rapport à l'an dernier.

Aucun appel manqué

Comme c'est le cas partout dans le monde, l'utilisation première du smartphone, pour les citoyens luxembourgeois, ne consiste plus à passer des appels.

Au quotidien, leur téléphone leur sert principalement à envoyer des e-mails (68 pour cent) et des SMS (65 pour cent) ainsi qu'à discuter par messagerie instantanée (58 pour cent). Seuls 42 pour cent des participants déclarent passer au moins un appel par jour.

«Une autre constatation intéressante est que les utilisateurs de smartphones au Luxembourg semblent utiliser leur téléphone beaucoup plus que leurs voisins européens. Le Grand-Duché est dans le top trois dans tous les domaines d'utilisation du smartphone, ce qui indique que les individus utilisent leur téléphone pour de nombreuses raisons différentes», explique **Georges Kioes** (cf. portrait), Partner et TMT Leader chez Deloitte Luxembourg.

Pas de téléphone à table

Si la population luxembourgeoise utilise activement les téléphones portables en journée, trois participants sur quatre déclarent laisser leur portable de côté lors d'un repas entre amis ou en famille. Néanmoins, cette tendance ne s'applique pas sur le lieu de travail car seules 33 pour cent des personnes interrogées disent éviter d'y utiliser leur téléphone portable.

Banque mobile

Au Luxembourg, les détenteurs d'appareils «intelligents» préfèrent encore utiliser leur ordinateur portable pour vérifier le solde de leurs comptes bancaires, mais le smartphone gagne du terrain dans ce domaine. Cette année, 28 pour cent des participants à l'enquête déclarent privilégier leur smartphone pour tenir leur compte à l'œil, contre 20 pour cent seulement en 2016.

Sur ce point, le Luxembourg reste toutefois derrière d'autres pays, dont les utilisateurs sont plus actifs. De même, le recours au smartphone pour les paiements en magasin reste rare au Grand-Duché. Là où 62 pour cent des utilisateurs danois payent via leur téléphone en magasin, moins d'un cinquième des participants luxembourgeois mentionnent avoir utilisé cette fonctionnalité.

«L'enquête montre qu'il existe un' immense potentiel pour les banques d'accélérer la banque mobile au Luxembourg. Le taux d'adoption du smartphone y est l'un des plus élevés en Europe ; pourtant, très peu d'utilisateurs ont recours à leur téléphone pour effectuer des opérations bancaires. Aujourd'hui, proposer une meilleure expérience aux usagers par le biais d'une banque mobile et d'applications de paiement devrait constituer une priorité aux yeux de la majorité des banques», explique Ronan Vander Elst, Partner chez Deloitte Luxembourg.

Implementing GDPR : Challenges and Recommendations

By Dean Mitchell, Associate Partner & Magali Van Coppenolle, Senior Consultant, Avantage Reply

Rapidly developing technological advances combined with new and innovative commercial uses of personal data and diverse differences in data protection standards across the European Union have served as the catalyst behind the shift from the Data Protection Directive (95/46/EC) to the General Data Protection Regulation (EU 2016/679 or 'GDPR'). GDPR is designed to give citizens more control over their personal data.

In a data-intensive financial industry, understanding and managing data as an asset while ensuring appropriate and adequate risk management frameworks are in place, is crucial to remain one step ahead of the regulation and the market. Across the Reply Group we have collected feedback from various financial institutions in relation to the implementation of the GDPR. The majority of our clients are making good progress with their planning and GDPR implementation. Having completed a gap analysis and defining requirements firms are now firmly in the process of implementing the defined solutions. With less than a year to go before the go live date, of May 25 2018, we look at the challenges that GDPR poses to the financial service industry. We also formulate some recommendations for implementation based on our own experiences.

Broader and more complex

The GDPR is much broader in scope and more complex than its predecessor, the Directive. Key principles of the Directive are strengthened, and a number of new regulatory elements are added. Two points in particular should focus the attention of compliance departments: the new accountability principle and the shift to a risk-based approach. The new Accountability Principle implies that the "burden of proof" now falls on regulated entities. In a nutshell, data controllers have to the double obligations of complying with the regulatory principles as well as of demonstrating compliance to the supervisory authorities.

Secondly, the GDPR also introduces a risk-based approach to data privacy. Data collection and data processing are now positioned as a "risk to the protection of natural persons" and much of the regulatory requirements are now approached through a risk based point of view. For compliance departments, this means introducing risk assessments for various data processing activities and linking this with presumably existing classification of data sensitivity.

What Challenges are Firms Experiencing?

Although there are many new regulatory requirements relating to GDPR, based on our clients experience and our own experience, we have briefly summarised three specific areas where firms may wish to focus their attention.

1. The rights strengthened or newly granted;
2. Data breach notification and accountability; and,
3. Consent.

New rights for customers and new obligations for firms

The Regulation aims to empower "individuals and give them control over their personal data", which it does so by granting several rights to data subjects, such as the right to access, the right to rectification, the right to restrict processing, the right to data portability as well as the right to erasure. The later has been popularly named "the right to be forgotten".

It is likely that, over time, data subjects will increasingly call upon their rights to be exercised through requests and firms must prepare in advance for an increase in requests to manage the data a firm holds. If they fall within the regulatory provisions, data controllers will have no choice but to positively respond to such requests. It is also important to note that the data controller's new responsibilities extend beyond their own organisation. For example, in the event that data that is subject to a successful request to rectify or erase , was made public by the data controller, he or she must notify others processing that same data of the request. Active management and efficient interfaces with customers, or data-subjects, will hence be crucial as request management becomes business-as-usual. As companies will not be allowed to charge fees for the processing of this type of data request one of the great challenges is how to design a system that is not only effective but also economical to run.

It is clear that the personal data life-cycle starts with the first interaction with the customer and ends sometime after data has been transferred to a third-party. This will bring data management teams to the front office, interacting with clients, and, at the other end, data management teams will have to build working relationships with third parties. Shifting the burden of responsibility to any service providers is also regulated. The guidance issued by the Article 29 Working Party stipulates that when an outsourcing agreement is in place the responsibilities for data portability must be allocated among the parties by means of a contract. This increased focus on active data management throughout the data life-cycle will also impact the volume, quality and accuracy of meta-data supporting those processes.

Better accountability in cases of data breaches

Personal data breaches earn much attention in the Regulation. Data controllers will now have to maintain an internal breach register. In addition, data processors and data controllers will have to comply with a general requirement to notify the supervisory authorities, within 72 hours of a data breach being identified. Under specific circumstances, data controllers must also notify individuals affected by such breaches. As cyberattacks were recently ranked one of the top risks for 2017 by risk professionals, firms will need not only to sustain investment levels in cybersecurity, but also holistically conceptualise the management of such risks. The substantial fines that are potentially imposed under the GDPR are an additional incentive for firms to elevate data security as a top priority. The human factor in accidental breaches can also not be discounted, and recent history shows that significant breaches caused by mishandling are severely judged by regulators.

Under specified circumstances, companies must also notify data breaches to customers affected by such a breach. In those cases, and given the sensitive nature of the topic in the media and public opinion, firms are likely to face reputational challenges. For listed companies, and based on past events, a market reaction may also ensue.

Consent is differentiated, specific and explicit. It can also be withdrawn at any time.

The GDPR's threshold for consent is high and probably constitutes one of the most challenging aspects of the Regulation. Getting consent right will be crucial for the usability of any data collected. Consent will only be valid when requested separately for each processing activity. Requests should be conveyed in a clear and "unambiguous" manner. In line with the newly introduced principle of accountability, data controllers will have to be able to demonstrate that consent was given in accordance with regulatory requirements, and not simply through box-ticking, forced or "omnibus" consent. As noted in our introduction, individual data subjects are also granted a new right, that of withdrawing consent to use or even hold data at any given time. Individuals must be notified of this new right at the time that consent is requested. Finally, the principle of valid consent, when coupled with data transfer to third parties, could become particularly tricky. Tools and processes will need to incorporate information on what parties has obtained consent and how other parties rely on that consent.

The issue of consent will pose important questions with respect to the handling of the existing stock of data as for those, consent has been given long before this upcoming regulatory regime. Though the Regulation stipulates that consents given prior to the coming into force of the GDPR may still be valid; there is still the possibility that for certain stocks of data, or parts of datasets, the existing consent would be judged insufficient for further processing.

Implementing GDPR: a Few Recommendations

The paradigm shift introduced by the GDPR implies wide-ranging changes, impacting all aspects of organisations. We have listed below a few reminders and recommendations to consider.

- Data management starts at the source.
  - o Review and adjust consent request processes according to new requirements;
  - o Ensure that all client-facing staff are aware of data management guidelines and can be of assistance to customers and data-management teams;
  - o Ensure user-friendliness of all customers' platforms and interfaces.

- Data and consent are managed across the organisation and throughout the data lifecycle.
  - o Assess your data management processes holistically;
  - o Design the company's request-handling process from end-to-end, with consideration for new types of interactions between data management teams, front and back offices as well as third parties;
  - o Manage data and consent actively and over time – not just during the GDPR project;
  - o Assess potential for leverage among processes for the handling of customers' data requests. 'Customer's preferences Centres' are examples of such efficient management of requests and consent;
  - o Review existing data stocks with respect to current consent and necessary consent as per the GDPR;
  - o Review accuracy of meta-data and the extent to which existing meta-data provides sufficient information for the compliant storage and processing of personal data.

- Technology can be your data management's best friend.
  - o Assess the capability of current underlying technology in dealing with data subjects' requests;
  - o Assess the capability of current underlying technology in supporting the necessary processing controls;
  - o Assess the potential for additional automation, for both internal data management and the handling of customers' requests.

- Design pro-active reactions to breaches.
  - o Update incident identification systems as well as internal and external breach notification procedures, as per regulatory requirements;
  - o Include breaches as a plausible risk within risk management systems;
  - o Design processes for external interactions, both for the reporting to regulatory authorities and for the handling of customers' complaints in case of breaches;
  - o Include the management of reputational risk in the incident response plans. This should include the capacity to provide reassurance to markets and customers in a swift and professional manner.

Finally, the GDPR is likely to have a financial impact. It is hence important to assess cost implications not just in the implementation phase but also beyond it, in order to adequately resource compliance.

Technology: a key Ally

In many aspects, the GDPR questions data management practices that are heavily reliant, in the banking sector, upon underlying fragmented technology. However, the question may not be whether or not technology is a piece of the implementation puzzle, but rather, what piece of technology suits your organisation better.

The journey to a more secure and efficient way of managing personal data starts with data-mapping, which must answer the question of how data is collected and then propagates through a company's systems. Based on that knowledge, data governance frameworks are devised and backed by adequate technology solutions. Data governance should address the question of the nature of data collected and processed as well as their levels of sensitivity, and how to manage this in a compliant manner. Data governance will also have to include the implementation and management of data security tools. Some of those tools, such as encryption and segregation, are more familiar to banks than others, such as pseudonymisation. Protection against data loss is key and likely to receive regulatory scrutiny.

Technology solutions to support data governance are widely available. They can be add-ons to larger ERP or more encompassing data management software. Each solution comes with its own set of pros and cons. IT solutions should be selected with a long term view and advance planning by firms will help to avoid implementing a solution in two stages – an interim tactical solution and a longer term strategic solution.

Conclusion

The new Data Protection Regulation is an important piece of regulation and a welcome one. This shift in paradigm, which gives the customer more control over the use and storage of personal data should compel companies to re-think their data protection compliance programmes and the importance of risk management. Active management throughout data lifecycles is key and likely to be more resource-intensive for companies. Finally, the heavy fine regime introduced by the GDPR will also ensure that this new regime is taken seriously. As several regulatory areas remain to be further defined through guidelines, the financial service industry will want to ensure proper representation to the supervisory authorities and the European Data Protection Board. With under a year to go to achieve compliance, GDPR is the hot topic in financial services firms at the moment. Its implementation will be challenging, but with the right tools and approach, certainly feasible.