SQUIRE PATTON BOGGS

Les bonnes résolutions RGPD des entreprises pour 2019

Ne dites pas	Mais dites plutôt
La compliance/conformité ça ne m'intéresse pas ; c'est une invention de bureaucrates pour empêcher de faire des affaires et de développer des produits innovants.	Il faudra que je m'adapte. C'est le prix à payer pour profiter de l'évolution technologique. Il faut transformer la conformité en atout: analyse et nettoyage de nos bases de données et documents papiers, intégration des équipes, rationalisation et harmonisation des processus, arguments éthique et commercial, produits sécurisants.
Les clients et consommateurs ne s'intéressent pas à la protection des données personnelles ; il leur importe seulement d'avoir des services à bas prix ou gratuits.	Les clients et consommateurs prennent progressivement conscience des risques et abus. La conformité (transparence, minimisation, légitimité, sécurité etc.) devient gage de qualité et un argument de vente.
Comme pour le bug de l'an 2000, on a beaucoup appréhendé la date du 25 mai 2018. Et pourtant il n'y a pas eu de révolution. A quoi bon se stresser maintenant ?	Depuis le 25 mai 2018, il y a eu un nombre accru de plaintes, de notifications de violation, une augmentation du montant des sanctions et même des actions de groupe. Ce n'est pas un sujet à prendre à la légère.
Ce que j'ai fait l'année dernière suffit.	La conformité au RGPD est un processus continu et évolutif.
Le RGPD ce n'est pas bien compliqué, il suffit de le lire.	La réglementation est plus compliquée qu'il n'y parait. En plus du RGDP il y a des lois locales complétant ses dispositions et des guides d'interprétation au niveau de l'UE et de chaque pays. De plus, il y a des interactions avec le droit du travail , de la santé publique, des communications…
Je vais tout déléguer à quelqu'un…y compris ma responsabilité.	Je peux déléguer le travail mais pas ma responsabilité. Je dois m'impliquer.
Je nomme une personne en interne ou externe qui soit en charge et basta cosi. Qu'elle se débrouille toute seule.	Personne ne peut assumer cette charge isolément. La conformité doit être mise en œuvre par les différents départements de l'entreprise et les pays dans lesquels elle opère. Il faut donc que le management soit formé et impliqué. La personne dédiée, spécialiste ou DPO, peut en revanche les assister en structurant un plan d'action, et travailler en collaboration avec un réseau de référents.
Je n'ai pas besoin d'un plan de gestion des violations de données. Il sera toujours temps d'agir dans l'hypothèse où un incident surviendrait. Mais c'est peu probable.	La question n'est pas « si » cela va m'arriver, mais « quand ». Une fois que cela arrive, les délais sont serrés, les questions complexes et le risque élevé pour l'entreprise. Il vaut mieux prévenir que guérir.
J'ai conscience que les personnes concernées ont des droits, mais, soyons sérieux, pourquoi faudrait-il les « gérer » ?	L'exercice par les personnes concernées de leurs droits peut s'avérer compliqué à gérer, surtout dans un délai de 30 jours. Les droits d'accès, en particulier, nécessite souvent d'analyser, compiler et expurger les documents avant de pouvoir les communiquer à la personne concernée. Je ferai mieux d'anticiper cela !
Je n'ai pas/plus d'argent pour la conformité.	Certains outils peuvent être développés en interne avec l'aide des autres départements. Il peut même y avoir des synergies avec d'autre projets de l'entreprise. Et puis la compliance permettra d'améliorer les bases de données et processus de l'entreprise, ce qui justifie un budget.
Mais qu'est-ce que je risque en cas de non-conformité ? Pas grand-chose, non?	Les sanctions des autorités de contrôle peuvent paralyser mon activité en m'interdisant d'exploiter les données ou impacter sérieusement ma solvabilité (avec des amendes allant jusqu'à 20 millions € ou 4% du chiffre d'affaire mondial). Je pourrais aussi être exposé à une responsabilité pénale ou des actions de groupe. Et si cela ne suffisait pas , la non-conformité peut affecter la réputation de l'entreprise

Si vous avez besoin d'aide, que ce soit en France, dans d'autres pays européens, ou dans vos relations avec des sociétés basées en dehors de l'UE, n'hésitez pas à avoir recours aux services de notre équipe internationale « Données Personnelles et Cyber-sécurité ». Votre contact en France est Stephanie Faber stephanie.faber@squirepb.com.

SQUIRE PATTON BOGGS

Organisations' GDPR New Year's Resolutions for 2019

Do Not Say	Do Say
Compliance does not interest me. It is an invention of bureaucrats to prevent doing business and developing innovative products.	I will have to adapt. This is the price to pay to profit from the technological evolution. Compliance must be turned into an asset: analysis and cleaning of our databases and paper documents, integration of teams, rationalisation and harmonisation of processes, ethical and commercial arguments, and secure products.
Clients and consumers are not interested in risks and abuses related to privacy – they prefer to have cheap or free services.	Clients and consumers are gradually becoming more aware of the risks and abuses brought about by technology. Compliance (transparency, minimisation, legitimacy, security, etc.) guarantees quality and is a selling point.
Some felt that 25 May 2018 was akin to Y2K. But there was no "big bang". What is the point of stressing now?	Since 25 May 2018, there has been an increased number of complaints, data breach notifications, sanctions and even class actions. Compliance is important!
What I did last year should be enough.	GDPR compliance is an ongoing and evolving process.
The GDPR is not that complicated, you just have to read it.	The new Regulation is complicated! In addition to the GDPR, there are local laws supplementing its provisions and guidelines at EU and country levels. Further, there are interactions with labour law, public health law, communications law, etc.
I will delegate the work and my responsibility as controller to someone (internally or externally).	I will be accountable and will be able to delegate part of the work, but not the responsibility. I need to be involved.
I will appoint someone internally or externally to manage compliance on his/her own.	No one can manage compliance on his/her own. Compliance has to be implemented by each department and jurisdiction where we have operations. To this effect, management needs to be trained and aware. The data protection specialist or DPO will assist, making sure an action plan is in place and will collaborate with a network of DP contacts
I do not need a breach response plan. I will respond to an incident should it occur. A breach is unlikely, anyway.	A breach incident will occur – it is just a matter of time. Once it occurs, I will need to respond quickly. With significant penalties and my organisation's reputation on the line, I should have a plan in place to respond to incidents.
I know that data subjects have rights, but why would I need to "manage" them?	Responding to DSARs can be quite complicated, especially within a 30-day period. Access rights, in particular, may involve a cumbersome review and redacting process before data is shared with the data subject. I had better anticipate this.
I do not have any money to spend on compliance!	Some tools can be developed internally with the help of other departments. There may even be synergies with other projects in the organisation. GDPR compliance will improve the databases and processes of the company. Explaining this to stakeholders may justify a budget.
Seriously, what is the risk of non-compliance? Very limited, I would say.	Sanctions by EU data protection authorities may prevent me from using the database I need for my core activities, or may even materially impair my financial soundness (as sanctions can go as high as €20 million or 4% of global turnover). In some cases, I may even incur criminal liability or face class actions. If this is not enough, non-compliance will have a negative impact on my organisation's reputation.

If you need assistance, in the EU or outside the EU, with your GDPR compliance programme, do not hesitate to contact a member of our Data Privacy & Cybersecurity team.

Your contact in France is Stephanie Faber, stephanie.faber@squirepb.com.