STEPHENSON HARWOOD

RGPD – compte à rebours

Quelles-sont vos obligations ?

Le Règlement Général sur la Protection des Données personnelles ("**RGPD**") entre en vigueur le **25 mai 2018** et introduit d'importants changements en matière de loi sur la protection des données dans toute l'Union européenne. En France, l'application de ce règlement européen sera accompagnée de la modification du dispositif législatif issu de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, avec un nouveau projet de loi sur la protection des données personnelles.

Les deux axes majeurs du RGPD sont le renforcement des obligations existantes d'une part, et la création de nouvelles obligations d'autre part. **Quelles sont les conséquences pour votre entreprise ?**

Pour assurer le respect de la nouvelle loi avant le 25 mai 2018, il est primordial pour les entreprises de :

- faire l'audit de leurs pratiques actuelles en matière de protection des données ;
- apprécier l'impact des changements introduits par la loi sur leur propre activité ; et
- prendre toutes les mesures nécessaires pour combler leurs lacunes le cas échéant

Par où commencer ?

Ici, par ce document qui développe huit points essentiels du RGPD. Les entreprises qui traitent des données personnelles devront réaliser un audit de leurs pratiques en la matière, ce qui permettra d'identifier les pratiques qui répondent aux nouvelles exigences et celles qui devront faire l'objet de modifications. Toute mesure doit être entreprise dès que possible pour assurer la pleine conformité d'ici **mai 2018**.

Les points clés à adresser par les entreprises sont :

- La modification des avis/notices de confidentialité (privacy notices) pour s'assurer qu'ils répondent aux nouvelles exigences.
- La revue des mécanismes de mise en œuvre de la responsabilité au regard des strictes sanctions applicables en cas de non-conformité.
- L'examen des fondements juridiques adoptés pour le traitement des données personnelles.
- La mise en place de délais plus courts pour respecter les demandes d'accès et signaler toute violation à la Commission nationale de l'information et des libertés ("**CNIL**").
- Le renforcement des droits nouveaux et existants des personnes sur leurs données personnelles.
- L'examen des accords conclus avec les tiers pour assurer la conformité avec les nouvelles exigences.
- Les négociations avec les fournisseurs de services sur l'étendue de leur responsabilité pour violation de la loi sur la protection des données et indemnité requise.
- La désignation d'un Délégué à la Protection des Données ("**DPD**") pour notamment assumer la mission de contrôle de la conformité juridique des traitements (en particulier, vis-à-vis de la CNIL), informer et conseiller l'entreprise, tout sous-traitant ou salarié. Le DPD devrait être un dirigeant ou un membre senior du management mais pourrait être également un délégué mutualisé ou externe à l'entreprise.

1. Information détenue par les entreprises

En vertu de la loi actuelle, les responsables du traitement des données sont implicitement tenus de bien connaitre la teneur des données qu'ils détiennent et conservent.

Le RGPD renforce cette exigence en imposant aux responsables des données d'enregistrer et de documenter les détails des données, y compris la nature des données qu'ils contiennent, les objectifs de leur traitement et les personnes avec qui ils les partagent. Les sous-traitants de données doivent également documenter leurs activités de traitement.

De cette manière, les entreprises peuvent découvrir certaines problématiques relatives à la protection des données qui devront être traitées. Par exemple, les responsables des données pourront identifier certaines données qui ne sont pas nécessaires et pourront prendre des dispositions pour leur suppression.

Pour se conformer à cette nouvelle exigence, il est conseillé aux entreprises de réaliser un audit des données couvrant :

- les données personnelles détenues
- la source de ces données
- le lieu, la durée et la méthode de stockage des données
- la(les) raison(s) pour laquelle il est nécessaire de traiter ces données
- la légitimité du traitement de ces données
- les personnes ayant accès aux données

2. Communication des informations confidentielles

A l'heure actuelle, les responsables du traitement des données sont déjà tenus d'utiliser des avis/notices de confidentialité (privacy notices) pour fournir des informations claires de traitement aux personnes concernées, telles que les employés et les clients, et pour demander à obtenir leur consentement exprès au traitement de données personnelles et sensibles.

Le RGPD renforce les obligations existantes et impose aux responsables du traitement des données de communiquer des informations supplémentaires aux personnes concernées, notamment :

- la(les) raison(s) et le fondement juridique sur lesquelles ils s'appuient pour traiter les données personnelles
- la durée de conservation des données personnelles
- les informations relatives au droit de porter plainte auprès de la CNIL lorsque les personnes estiment qu'il y a un problème de traitement de leurs données

Tous les avis doivent être clairs, précis, intelligibles et aisément accessibles.

Les responsables du traitement des données devront revoir les avis/notices de confidentialité existants et les mettre à jour conformément aux nouvelles exigences.

3. Droits sur les données (incluant les demandes d'accès)

La loi actuelle sur la protection des données accorde d'ores et déjà certains droits aux personnes dont les données personnelles sont détenues par le responsable du traitement, notamment le droit d'accès et le droit de mettre fin à certains traitements de données.

Le RGPD apporte des améliorations et des ajouts significatifs à ces droits existants, notamment un nouveau droit de suppression des données personnelles lorsque la poursuite du traitement est inutile (et non plus seulement lorsqu'un dommage ou un préjudice serait causé) ainsi qu'un droit à la "portabilité des données", la capacité de demander le transfert de données vers un autre responsable de traitement.

En outre, les exigences de la demande d'accès aux données sont renforcées, de sorte que :

- Le délai de réponse à toute demande d'accès aux données est d'un (1) mois.
- Il est possible de refuser, ou de demander des frais d'administration raisonnables pour des demandes d'accès de données non fondées ou vexatoires, mais les informations requises doivent néanmoins être fournies à la personne concernée dans de telles circonstances.

Les entreprises devront examiner leurs procédures pour se conformer à ces droits renforcés.

4. Consentement du propriétaire des données

Le consentement au traitement des données personnelles deviendra généralement plus difficile à obtenir. Il devra désormais être donné librement, explicitement, de manière informée et sans ambiguïté. Il sera soumis à une déclaration positive (opt-in) et par conséquent le silence, les cases pré-cochées ou l'inactivité ne pourront donc plus valoir acceptation. Les demandes de consentement regroupées avec d'autres termes, et non clairement séparées, ne sont pas garanties comme suffisantes au regard du RGPD.

Les responsables du traitement qui se basent sur le consentement pour traiter les données devront revoir les consentements existants pour déterminer s'ils seraient adéquats au regard du RGPD ou s'il y existe des motifs juridiques plus appropriés sur lesquels se fonder.

Les avis/notices de confidentialité existants dans les contrats clients peuvent ne pas être adéquats et un nouveau mécanisme de consentement conforme au RGPD pourrait donc être requis.

Toute personne concernée devra pouvoir retirer son consentement à tout moment, ce qui pourrait créer des problèmes opérationnels importants pour les responsables de traitement. Un consentement conforme au RGPD pourrait, de plus, être difficile à obtenir par les employeurs auprès de leurs employés, compte tenu du déséquilibre de pouvoir qui empêche de considérer le consentement comme ayant été

donné librement. Il sera ainsi probablement nécessaire pour les responsables de traitement de rechercher un fondement juridique différent pour traiter ces données personnelles.

5. Fondement juridique pour le traitement des données personnelles

Le ou les fondements juridiques adoptés pour le traitement des données personnelles poseront davantage de difficultés dans le cadre du RGPD, car certains droits des personnes seront modifiés en fonction du fondement juridique adopté. Par exemple, si les responsables de traitement se fondent sur le consentement, les personnes concernées auront généralement des droits plus étendus, y compris le droit de voir leurs données supprimées.

Les alternatives au consentement des personnes concernées pour les données personnelles sensibles comprennent les cas où le traitement est nécessaire à l'exécution d'un contrat avec la personne concernée ou aux fins d'intérêts légitimes poursuivis par le responsable du traitement (sauf lorsque ces intérêts sont outrepassés par les intérêts, droits ou libertés de la personne concernée).

Les responsables du traitement des données doivent déterminer le fondement juridique sur la base duquel les données personnelles sont traitées, les documenter et mettre à jour les avis/notices de confidentialité pertinents pour les expliquer.

6. Responsabilisation - Démontrer la conformité

Le RGPD inclut un principe de responsabilité, ce qui signifie que les entreprises doivent non seulement se conformer aux principes de protection des données mais aussi démontrer comment elles s'y conforment.

De nombreuses mesures existent pour garantir et démontrer sa conformité :

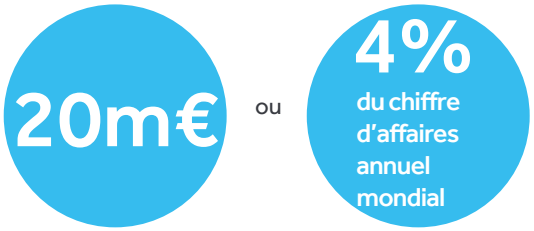
- Enregistrer toute activité de traitement des données effectuée dans un registre dédié.
- Mettre en œuvre (ou revoir) les mesures techniques et organisationnelles telles que les politiques de protection des données sur la formation des employés et les audits internes des activités de traitement.
- Effectuer une étude d'impact de la protection des données ("EIPD") si le traitement des données est susceptible d'entraîner un risque élevé pour les individus, par exemple lorsqu'une nouvelle technologie est utilisée. Les responsables de traitement peuvent préparer un document/ modèle EIPD.
- Prendre des mesures qui respectent les principes du "*privacy by design*" et du "*privacy by default*", notamment la minimisation des données, la pseudonymisation, la transparence et l'amélioration continue des fonctionnalités de sécurité.

7. Infractions et amendes pour violation

Une violation de la protection des données personnelles est une violation de la sécurité conduisant à la destruction, la perte, la modification, la divulgation ou l'accès non autorisés à des données personnelles.

Les responsables de données seront désormais tenus de notifier toute violation à la CNIL lorsqu'il y aura un risque d'atteinte aux droits et libertés des individus (par exemple lorsqu'une violation sera susceptible d'entraîner une discrimination, une atteinte à la réputation ou un préjudice financier). Les notifications doivent être effectuées sans retard injustifié et, si possible, dans les 72 heures suivant la prise de connaissance de la violation. Si la violation est susceptible d'entraîner un risque élevé aux droits et libertés des individus, le responsable du traitement doit également informer les personnes concernées directement et sans retard injustifié.

Le défaut de notification peut entraîner une amende pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial annuel. En outre, des amendes plus élevées peuvent être imposées pour la violation elle-même, qui pourront aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial annuel (une augmentation significative de la sanction pécuniaire actuelle d'un montant maximal de 150 000 € et de 300 000 € en cas de récidive).



La responsabilité potentielle des responsables de traitement est donc fortement accrue. Les sous-traitants exploitant des données personnelles, tels que les fournisseurs tiers, ont, en vertu du RGPD, la responsabilité directe d'informer le responsable du traitement "sans retard injustifié" après avoir pris connaissance d'une violation de la protection des données personnelles. Cependant, les responsables de traitement sont libres de rendre cette obligation plus contraignante contractuellement, par exemple en exigeant que le sous-traitant concerné les notifie dans les 24 heures, pour leur permettre de respecter le délai de 72 heures.

Les responsables du traitement doivent s'assurer d'avoir des procédures robustes pour identifier, évaluer, enregistrer et, le cas échéant, notifier les violations. Les responsables du traitement peuvent également revoir les mécanismes de protection contre la responsabilité à travers des garanties dans leurs contrats avec les sous-traitants et leurs assurances de responsabilité civile.

8. Contrats avec les sous-traitants exploitant des données

Le RGPD impose des obligations juridiques directement sur les sous-traitants amenés à exploiter des données personnelles en matière notamment de mise en œuvre de mesures appropriées de sécurité des données et de tenue d'un registre des traitements effectués pour le compte d'un responsable de traitement des données. Ces sous-traitants sont également tenus de s'assurer que les contrats avec les responsables de traitement contiennent certaines stipulations minimum, telles qu'une description de l'étendue, de la nature et de l'objectif du traitement.

Les responsables de traitement doivent revoir et mettre à jour leurs contrats avec les sous-traitants amenés à exploiter des données personnelles afin de s'assurer qu'il existe des stipulations appropriées concernant les nouvelles obligations directes de ces sous-traitants et les autres sujets importants tels que la conformité, la surveillance et l'information.

Il est également nécessaire de revoir les clauses de responsabilité et d'indemnisation dans les contrats afin de s'assurer que la répartition des risques reste appropriée au regard des nouvelles obligations juridiques directes des sous-traitants et des responsabilités partagées des responsables de traitement de données et des sous-traitants dans des domaines tels que la sécurité.

Les sous-traitants seront directement responsables de toute violation du RGPD et pourront, en conséquence, envisager de demander une indemnisation auprès des responsables de traitement pour les amendes imposées du fait desdits responsables de traitement.

Pour de plus amples informations sur les développements relatifs au RGPD, pour obtenir un conseil en protection des données ou sur tout autre sujet s'y rapportant, nous vous invitons à contacter nos avocats ci-dessous.

Indranee Dursun

Collaboratrice sénior, Paris

T: +33 1 44 15 80 05
E: indranee.dursun@shlegal.com

Jonathan Kirsop

Associé, Londres

T: +44 20 7809 2121
E: jonathan.kirsop@shlegal.com

BD405-GDPR-0418