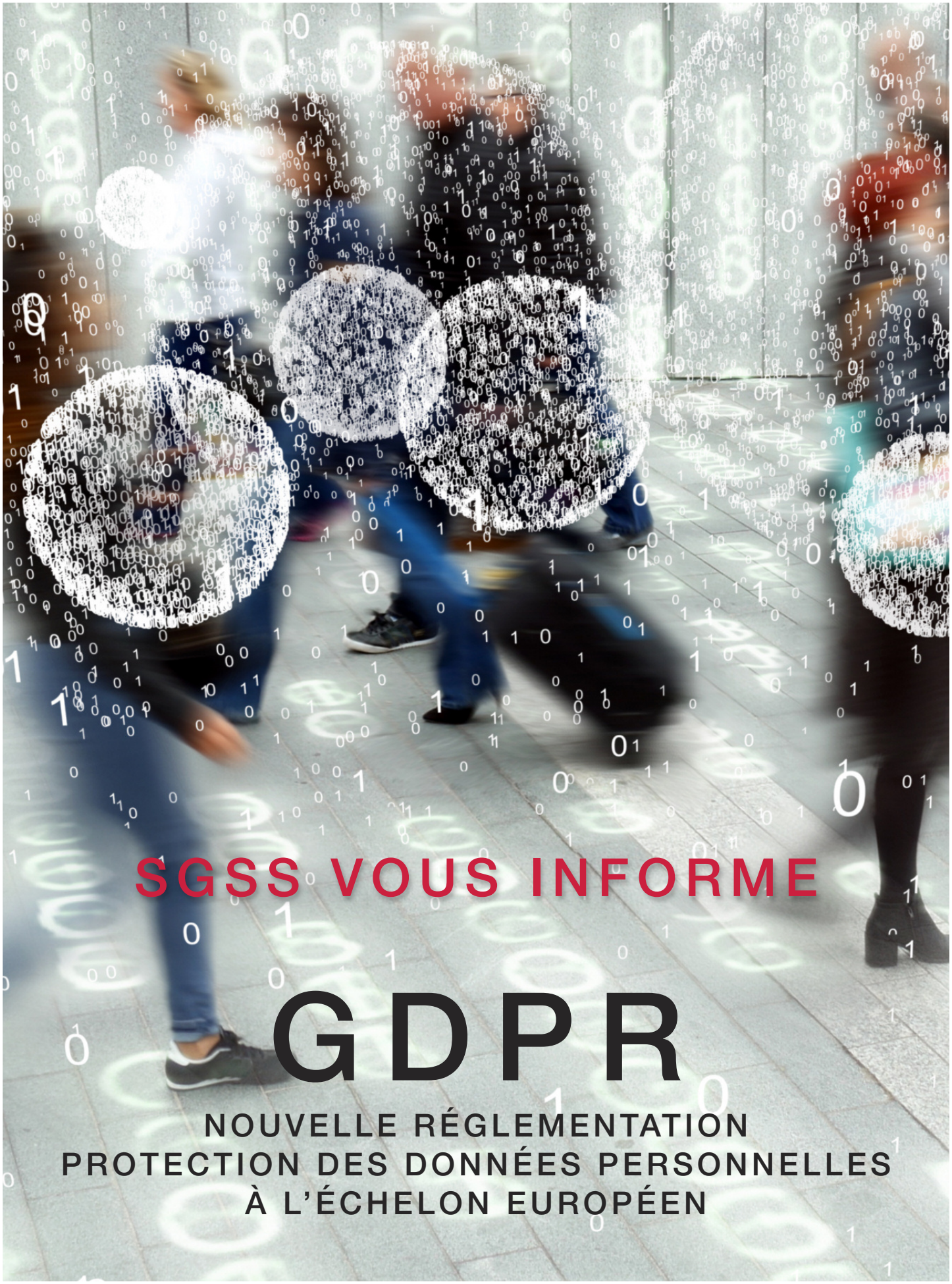

SGSS VOUS INFORME

GDPR

NOUVELLE RÉGLEMENTATION PROTECTION DES DONNÉES PERSONNELLES À L'ÉCHELON EUROPÉEN

SOCIETE GENERALE
Securities Services

DEVELOPPONS ENSEMBLE
L'ESPRIT D'EQUIPE

VOUS ÊTES CONCERNÉ

La révolution digitale a fait exploser le nombre de data générées dans le monde. Face à la multiplication des utilisations de données personnelles dans l'ensemble des secteurs économiques et en réponse aux inquiétudes exprimées par les citoyens européens, le législateur européen, sous l'inspiration des autorités de supervision, a publié le règlement GDPR : General Data Protection Regulation (ou RGPD : Règlement Général de Protection des Données). Adopté le 27 avril 2016, ce règlement européen entrera en vigueur le 25 mai 2018.

DONNÉE PERSONNELLE : DÉFINITION

Les données à caractère personnel sont définies comme « toute information relative à une personne physique identifiée ou identifiable (…), directement ou indirectement, par référence à un identifiant (nom, numéro d'identification) ou à un ou plusieurs éléments spécifiques propres à son identité physique, …, économiques, sociales, »*
Il peut s'agir de données clients mais aussi de données collaborateurs, prestataires, partenaires, actionnaires, …

* Extrait GDPR Article 4

General Data Protection Regulation

QUELS OBJECTIFS POUR GDPR ?

GDPR **renforce la réglementation existante** (Directive 95/46/EC) sur **la protection des individus,** de leurs données personnelles et vise également à **préserver leur identité numérique. Enfin,** Il a vocation à **harmoniser les règles de protection des données personnelles entre tous les pays européens.**

LES 3 OBJECTIFS DE GDPR À LA LOUPE

■ **Renforcer le droit des individus et la maîtrise de leurs données personnelles**

- Recueil obligatoire **d'un consentement** explicite pour des usages non prévus au contrat
- **Transparence** de l'information au client sur l'usage de ses données, **droit d'accès et de rectification**
- **Droit à l'oubli** élargi aux données du Web
- **Droit à la portabilité** offrant la possibilité de récupérer ses données pour pouvoir les réutiliser ou les transmettre à un tiers
- **Protection** particulière **pour les mineurs.**

■ **Augmenter la responsabilité des acteurs traitant des données**

- Tenue d'un **registre des traitements** mis en œuvre par le **Responsable des traitements**
- Désignation d'un **Délégué à la protection des données (DPO)**
- Mise en œuvre de **la sécurisation dès la conception (Privacy by design),** reposant sur la minimisation des données collectées, la limitation de leur usage à l'objet initial et leur suppression dès lors que les délais de conservation légaux sont éteints.
- Réalisation **d'études d'impacts de la vie privée**
- Notification en cas de **fuite ou violation de données personnelles,** sous 72 heures, à l'autorité de contrôle et le cas échéant au propriétaire des données
- Encadrement strict de la **sous-traitance,** afin de garantir la chaîne de conformité de bout en bout.

■ **Crédibiliser la réglementation,** sous l'autorité du Comité Européen de Protection des Données, grâce à une coopération renforcée entre les autorités de protection des données et un guichet unique dans le pays de résidence pour les opérations transfrontières (CNIL en France) et des sanctions renforcées.

General Data Protection Regulation

QUI EST CONCERNÉ PAR GDPR ?

GDPR s'applique à **toutes les entreprises,** quels que soient leur taille ou leur secteur économique et où qu'elles soient établies, qui collectent, hébergent, traitent les **données personnelles des résidents et ressortissants de l'Union Européenne.**

LES SANCTIONS PRÉVUES

GDPR prévoit des **sanctions financières graduées** allant jusqu' à 20 M€ ou 4% du chiffre d'affaires en cas de manquement grave aux principes fondamentaux du texte.

A noter qu'avec l'entrée en vigueur depuis Octobre 2016 de certaines dispositions de la loi pour la République numérique (loi Lemaire), le montant maximal des sanctions- auparavant fixé à 150 k€ -a été porté à 3 M€.

General Data Protection Regulation

QUELLE FEUILLE DE ROUTE POUR LES ENTREPRISES ?

La première étape est un **diagnostic complet sur les traitements** impliquant des données personnelles Savoir quelles données sont concernées, où elles sont conservées, qui les exploitent, qui peut y accéder permet d'évaluer concrètement l'impact de GDPR sur votre entreprise. L'élaboration d'un **registre des traitements** aide à ce diagnostic.

Ensuite, il convient de **définir les actions à engager : nomination d'un DPO (Délégué à la protection des données), revue des process,** amélioration des **outils informatiques, audit de sécurité,** renforcement des contrôles, revue des relations avec les sous-traitants, formation des collaborateurs, …

Ces travaux faisant appel à plusieurs compétences, il convient de se mobiliser sans retard pour les mener à bien d'ici à mai 2018.

Le message envoyé aux entreprises concernées par GDPR est qu'il est désormais encore plus impératif de traiter les données à caractère personnel avec un soin tout particulier et beaucoup de rigueur. Au-delà de la mise en conformité avec la réglementation, c'est pour chaque entreprise un enjeu d'image et de réputation auprès de ses clients.

En savoir plus : **https://www.cnil.fr/se-preparer-au-reglement-europeen**
http://www.eugdpr.org/