SUD NORD JOINTURE AVOCAT

CABINET SNJ AVOCAT
222, boulevard Saint-Germain
75007 Paris
contact@snj-avocat.fr

SUD NORD JOINTURE AVOCAT

LES ENJEUX DU DPIA A L'AIR DU BIG DATA

Instauré par l'article 35 du RGPD, le DPIA « ***Data protection impact Assessment*** » ou PIA « ***Protection Impact Assessment*** » oblige désormais, les organismes qui opèrent des traitements de données personnelles jugés à risque, à conduire une étude sur les impacts néfastes possibles sur la vie privée et les droits et libertés des personnes concernées.

En effet, à l'air de la transformation numérique et du Big Data, nos données personnelles sont entièrement dématérialisées. Collectées en ligne, elles transitent via internet (wifi, objets connectés etc.) et sont stockées sur des serveurs dont on sait souvent peu des mesures de sécurité réellement déployées.

La quantité de données produites chaque jour représenterait près de 2,5 trillions d'octets. Si la donnée constitue le nouvel «**el dorado**» pour les entreprises, les problématiques sécuritaires accompagnant ce contexte sont réelles.

De nombreux cas de violation de nos données personnelles dus à des attaques informatiques au sein de grands groupes ont été mis en lumière.

Ainsi, Yahoo en 2016, annonce avoir subi une cyber-attaque (en 2013) ayant impacté l'ensemble de **ses 3 milliards de comptes utilisateurs**. Le géant du réseau social professionnel, LinkedIn révèle en 2016, que plus de **100 millions d'identifiants d'utilisateurs et de combinaison de mots de passe** ont été dérobés (en 2012), du fait d'une faille de sécurité dans ses systèmes.

Si on estime à plus de 400 millions d'euros par an le coût des cyber-attaques pour les entreprises (*source : McAfee et CSIS en 2016*), **quel est le coût pour la vie privée et les droits et libertés des personnes affectées ?**

« Le RGPD oblige désormais, les organismes à mesurer les impacts des traitements jugés à risque, sur la vie privée des personnes concernées »

L'article 35 du RGPD instaure à la charge des organismes la conduite d'une analyse d'impact sur la protection des données (DPIA ou PIA) dès lors qu'un traitement envisagé « ***est susceptible d'engendrer un « RISQUE ELEVE » pour les droits et libertés des personnes concernées*** ».

QUAND DOIT-ON MENER UNE ANALYSE D'IMPACT ?

Lorsque les traitements que vous envisagez ou mettez en œuvre remplissent **au moins deux des critères énumérés** ci-dessous vous devez obligatoirement procéder à une analyse d'impact.

@ L'évaluation d'aspects personnels ou notation d'une personne (ex : scoring financier, profilage) ;

@ La prise d'une décision automatisée ;

@ La surveillance systématique de personnes (ex télésurveillance) ;

@ Le traitement de données sensibles (race, santé, biométrie, religion..) ;

@ Le traitement de données relatives à des personnes vulnérables (ex mineurs) ;

@ Le traitement à grande échelle de données personnelles ;

@ Le croisement d'ensembles de données ;

@ Des usages innovants ou l'application de nouvelles technologies (ex objets connectés) ;

@ L'exclusion du bénéfice d'un droit, d'un service ou contrat (ex listes noires).

EN QUOI CONSISTE L'ANALYSE D'IMPACT ?

Le PIA consiste pour le responsable du traitement à évaluer le niveau de risque du traitement envisagé ou mis en œuvre sur la vie privée des personnes concernées, par l'élaboration d'un scénario hypothétique répondant à l'interrogation suivante :

*Comment une **source de risque** (concurrents, salarié corrompu...) pourrait-elle exploiter les vulnérabilités **des supports de données** (base des fichiers clients par ex)*

dans le cadre de ***menaces*** *(détournement, vol, accès illégitime) sur les données à caractère personnel (fichiers clients) et provoquer* ***des impacts sur la vie privée*** *des personnes concernées (escroquerie à la carte bancaire, atteinte vie privée) ?*

Le risque sera apprécié en terme de : **gravité/ Vs vraisemblance**

⇒ *Quel peut être l'ampleur du préjudice pour l'individu ?* ***(sa gravité)***
⇒ *Quelles sont les chances que le risque se réalise ?* ***(la Vraisemblance).***

Après avoir analysé les mesures déjà existantes ou prévues dans l'entreprise et contribuant à la sécurité des traitements, (chiffrement des données, sécurité des exploitations, mesures organisationnelles), le responsable du traitement devra mettre en exergue les causes et conséquences de chaque événement redouté en analysant leur vraisemblance.

La vraisemblance sera essentiellement estimée au regard de la **vulnérabilité des supports** concernés et de la **capacité des sources de risques à les exploiter**.

Si les risques ainsi identifiés sont jugés acceptables ou limités au regard des mesures existantes ou prévues : le PIA est concluant et le traitement peut être envisagé.

Dans le cas contraire, des mesures complémentaires doivent être mises en œuvre afin de déterminer les risques résiduels.

QUELLE EST LA METHODE POUR PROCEDER A UNE ANALYSE D'IMPACT ?

Le responsable du traitement est libre de choisir sa méthode d'évaluation dès lors que celle-ci respecte les critères définis dans l'annexe 2 des lignes directrices du G29.

Les guides de la CNIL (*https://www.cnil.fr/fr/PIA-privacy-impact-assessment*) préconisent la méthode suivante :

⇒ **Délimiter et décrire le contexte** du (des) traitement(s) considéré(s) ;
⇒ **Analyser les mesures** garantissant le respect des principes fondamentaux : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;
⇒ **Apprécier les risques** sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;
⇒ **Formaliser la validation** du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

A QUEL STADE DU TRAITEMENT UN DPIA DOIT-IL ETRE ENVISAGE ?

L'analyse d'impact doit être menée **le plus en amont possible,** dès la conception d'un nouveau traitement. Elle doit s'inscrire dans une démarche itérative afin de parvenir à un dispositif de protection de la vie privée acceptable et doit être mise à jour dès qu'une évolution significative a lieu.

QUELS SONT LES ACTEURS IMPLIQUES DANS UN DPIA ?

En premier lieu, le Responsable du traitement.

Si celui-ci a désigné un Délégué à la protection des données, il pourra le charger de vérifier sa bonne exécution. Les sous-traitants s'il en existe, doivent également prêter main forte en fournissant toutes les informations nécessaires à la réalisation du PIA.

Le Responsable du traitement devrait par ailleurs faire participer au processus de réalisation, les équipes de son organisation impliquées dans la mise en œuvre du traitement (maîtrise d'œuvre et d'ouvrage, RSSI, etc.) et consulter les personnes concernées.

FAUT-IL TRANSMETTRE SON DPIA A LA CNIL ?

En principe le PIA ne doit être transmis à la CNIL que dans certains cas. Il doit ainsi, être obligatoirement transmis :

⇒ S'il apparaît qu'au terme de l'analyse, le niveau de risques résiduels demeure élevé (cas où la CNIL doit être consultée) ;
⇒ Quand la législation d'un Etat membre l'exige ;
⇒ En cas de contrôle de la CNIL.

QUELLES SANCTIONS EN CAS DE MANQUEMENT ?

Tout responsable de traitement qui enfreint l'obligation de mener un DPIA dans le cadre de la mise en œuvre d'un traitement susceptible « ***d'engendrer un RISQUE ELEVE » pour les droits et libertés des personnes concernées »***, encourt une amende pouvant aller jusqu'à 10.000.000 € ou dans le cas d'une entreprise jusqu'à 2 % de son CA mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Les entreprises ont donc désormais tout intérêt à se mettre en règle et entamer pour les traitements concernés leur analyse d'impact.