Gabin Courdy  
BTS SIO 1

Synthèse données à caractère personnel

[*Qu'est ce qu'une donnée à caractère personnel ?*](#_Toc1)

[*Qu'est ce qu'une donnée sensible ?*](#_Toc2)

[*Qu'est ce que le RGPD ? Donnez ses objectifs et où s'applique-t-il ? Donnez ses 5 grands principes et les sanctions prévues.*](#_Toc3)

[*Qu'est ce qu'un traitement des données ? Que doit avoir ce traitement pour être en accord avec le RGPD ?*](#_Toc4)

[*Quelles sont les obligations que doivent respecter les organisations pour être en conformité avec le RGPD ?*](#_Toc5)

[*Quels sont les droits accordés aux internautes, aux personnes afin de maîtriser leurs données personnelles ?*](#_Toc6)

[*Qu'est ce que la CNIL ? Donnez ses missions ?*](#_Toc7)

[*- Présentez les 6 principes qu'une entreprise doit respecter pour que sa charte de confidentialité soit en accord avec la protection des DCP*](#_Toc8)

Qu'est ce qu'une donnée à caractère personnel ?

Selon la CNIL : *Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable.*

Une donnée à caractère personnel permet donc d’identifier un individu. C’est ce qui fait sa valeur et la nécessité de protéger et réglementer l’usage de telles données.

Qu'est ce qu'une donnée sensible ?

Une donnée sensible compte aussi comme donnée personnelle. Elle permet d’identifier un individu. Mais elle permet en plus de le discriminer. Une donnée sensible peut révéler la religion, l’opinion politique, l’origine ethnique, raciale, la localisation, la condition médicale et d’autres données biométriques, de l’individu.

Un exemple de donnée sensible quotidiennement communiquée est le dossier médical d’un individu, retransmis entre les professionnels de santé, ou d’autres données médicales d’un scolaire communiquées à son établissement scolaire.

Qu'est ce que le RGPD ? Donnez ses objectifs et où s'applique-t-il ? Donnez ses 5 grands principes et les sanctions prévues.

Le RGPD est le Règlement Général de Protection des Données. Ce règlement européen encadre la collecte, le traitement et la sécurisation des données personnelles des citoyens de l’Union Européenne. Il s’applique à toute entreprise au sein de l’Union Européenne, et à toute entreprise au monde traitant les données de citoyens européens.

* Accountability : L’entreprise doit pouvoir démontrer officiellement qu’elle respecte le RGPD.
* Privacy by design : Le respect de la confidentialité des données est inclus dans la conception de l’application.
* DPO : Délégué à la Protection des Données, veille au respect du RGPD et sert de contact aux autorités.
* Security by default : La sécurité est incluse dans la conception de l’application, et le système d’information de l’entreprise est sécurisé à tous les niveaux, du logique au physique.
* Etude d’impact : analyse d’impact d’atteintes potentielles à la protection des données dès la mise en œuvre de nouveaux traitements des données.

L’irrespect d’un seul de ces principes est sanctionnable d’amendes, 800 000 euros ou bien et des réparations dont le prix varie selon la gravité de la violation.

Qu'est ce qu'un traitement des données ? Que doit avoir ce traitement pour être en accord avec le RGPD ?

Un traitement de données est le traitement de données générées par un client. Ce traitement doit avoir une finalité non abusive, légitime et être inscrit dans le registre des traitements de données.

La CNIL résume en cinq principes la conformité d’un traitement :

* Tout traitement doit se fonder sur une base légale, qu’on peut définir comme le droit, ce qui autorise l’entreprise, à traiter des données personnelle. Chaque finalité doit reposer sur une unique base légale. C’est le principe de finalité.
* Les données doivent être aussi pertinentes et réduites au strict nécessaire pour l’accomplissement de la finalité. C’est le principe proportionalité et pertinence.
* Les données traitées ne seront pas conservées indéfiniment. C’est le principe de conservation limitée.
* La sécurité et la confidentialité doit être garantie par le responsable du fichier, et seules les personnes autorisées sont censées avoir accès au fichier. C’est le principe de sécurité et confidentialité.
* Enfin, le traitement doit respecter le droit des personnes en les informant de la finalité de la collecte de leurs données et de comment exercer leurs droits.

Quelles sont les obligations que doivent respecter les organisations pour être en conformité avec le RGPD ?

Les obligations impliquées par le RGPD sont de plusieurs ordres :

* Sécurité et confidentialité, suivies par le responsable du traitement des données, en fixant :
  + des mesures de sécurité des locaux et des systèmes d’information
  + une durée de conservation raisonnable des informations personnelles
* Information, suivie par l’entreprise détenant les données personnelles, en rensiegnant :
  + l’identité du responsable du fichier
  + la finalité du traitement des données
  + si les réponses sont obligatoires ou optionnelles
  + les droits d’accès, de rectification, d’interrogation, d’opposition
  + la portabilité des données
  + la collecte de données
  + le rapport des données collectées avec la finalité du traitement
* Légalité :
  + les données ne peuvent être transférées hors Union Européenne si un niveau de protection suffisant n’est pas assuré
* Administration :
  + toute organisation de plus de 250 salariés doit tenir un registre des activités des traitements, à moins que ces traitements ne soient qu’occasionnels.

Le délégué à la protection des données (DPO) doit lui-même respecter ses propres obligations :

* informer et conseiller le responsable du traitement des données
* Assurer le respect du droit français et du règlement européen dans la protection des données
* Conseiller l’organisation à propos de l’analyse d’impact et vérifier cette analyse

Quels sont les droits accordés aux internautes, aux personnes afin de maîtriser leurs données personnelles ?

Les internautes peuvent exercer trois droits, et porter plainte contre l’entreprise en case de violation. Les sanctions peuvent être des réparations, une amende vingt millions d’euros ou quatre pourcents du chiffre d’affaire...

* Droit à la portabilité : récupération sous format exploitable et lisible sur tout ordinateur de ses données
* Droit à l’oubli : effacement et/ou déréférencement de ses données
* Droit à la notification : être averti rapidement par le responsable du traitement en cas de violation à haut risque de la sécurité données. La CNIL, qui catalogue publiquement les violations dangereuses, devra aussi être notifiée dans les soixante-douze heures.

Qu'est ce que la CNIL ? Donnez ses missions ?

La CNIL est une autorité administrative indépendante, composée d’un Collège de 18 membres et d’une équipe d’agents contractuels de l’État. Sa création remonte à 1978, engendrée par la loi Informatique et Libertés. La CNIL est investie de quatre missions :

* Informer : Communication et information des personnes
* Conseiller : Aider à se conformer au RGPD
* Innover : La CNIL organise des débats et expositions de nouvelles solutions de sécurité et de l’avenir des traitements de données
* Contrôler et sanctionner : La CNIL contrôle des entreprises et les flux de données retransmises selon les problématiques du moment et prononce des sanctions envers qui déroge au RGPD

Présentez les 6 principes qu'une entreprise doit respecter pour que sa charte de confidentialité soit en accord avec la protection des DCP

* Limiter la collecte des données au nécessaire : les données sont collectées selon une finalité bien déterminée et légitime. On parle aussi de principe de minimisation.
* Transparence : La maîtrise des données revient aux clients. Les personnes doivent être informées de leurs droits, et de comment les exercer.
* Facilitation de l’exercice du droit des individus : Aucune stipulation compliquant les modalités de l’exercice du droit des personnes n’est permise.
* Conservation définie : Les données traitées ne peuvent être indéfiniment stockées. Elle doivent être ultimement détruites. Si les données présentent un intérêt légal ou historique, elles doivent être anonymisées ou archivées comme toute archive publique, selon les applications légales impliquées.
* Sécurité : Les données doivent être stockées dans un environnement sécurisé. Cela implique la sécurité logique et matérielle (informatique), et du local utilisé.
* Conformité dynamique : Les traitements doivent être constamment surveillés, afin de s’assurer qu’ils restent conformes, et les techniques de sécurité mises à jour.