

Paris

Lyon

Marseille

Rennes

Face aux nouvelles contraintes réglementaires, à quelles conditions garantir conformité et sécurité des data ?

Henri LEBEN
Avocat associé - Groupe Colbert

L'entreprise, acteur et régulateur dans la collecte des données

- ⇒ Ne peut pas collecter n'importe quelle donnée
- ⇒ Doit mettre en garde la personne concernée
- ⇒ Doit accompagner la personne concernée dans sa gestion des données
- ⇒ Doit collaborer avec les autorités de contrôle

Paris

Lyon

Marseille

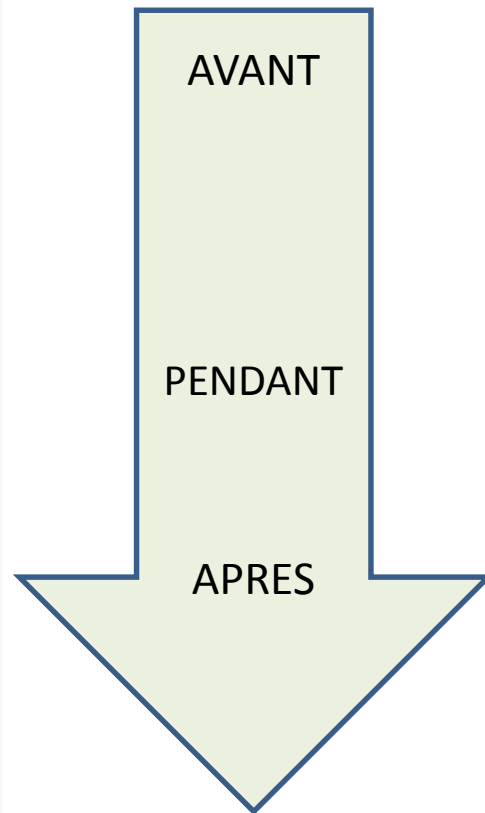
Rennes

Doit respecter / et démontrer qu'il respecte

3 niveaux de conformité

1. Conformité juridique
2. Conformité technique
3. Conformité organisationnelle

Conformité juridique



- Le traitement peut-il être mis en œuvre? (licéité du traitement, nature des données collectées, cas spécifique de l'étude d'impact) ;
- Respect de la réglementation lors de la collecte (formalisme plus important)
- Obligations post collecte

AVANT: Faut-il déclarer?

- Fin du régime de déclaration préalable
- Tenue d'un registre
- Analyse d'impact et consultation préalable
v. Autorisation

Tenue d'un registre

- Au moins 250 salariés...sauf si le traitement
 - ✓ est susceptible de comporter un risque pour les droits et libertés des personnes concernées, **OU**
 - ✓ **n'est pas occasionnel** , **OU**
 - ✓ Données articles 9 et 10

(Art. 30)

Tenue d'un registre

Pseudonymisation

Chiffrement

- Caractéristiques du traitement +
- « dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 ».

Moyens permettant de garantir la confidentialité

Comment rétablir les données

Procédures de test...

L'analyse d'impact et la consultation préalable: un mécanisme plus protecteur et plus souple?

Considérants 89 et suivants

« Lorsqu'un type de traitement, **en particulier par le recours à de nouvelles technologies**, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.». (Art.35)

L'analyse d'impact et la consultation préalable

L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, **en particulier**, requise dans les cas suivants:

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;
- Données article 9

Liste établie par l'autorité de contrôle?

L'analyse d'impact n'implique pas automatiquement la consultation préalable de la CNIL

« Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement **lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque** ».
(Art. 36)

Pendant: comment recueillir le consentement?

Nécessité d'un acte positif ?

Article 7.1

« Dans le cas où le traitement repose sur le consentement, le responsable du traitement est en mesure **de démontrer** que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant »,

Démonstration du consentement:

Pour bénéficier de nos services, indiquez,

- **Une adresse email valable**
- **Un mot de passe**

Acte positif?

Mentions Informatique et Libertés

OU?

Pour bénéficier de nos services, indiquez,

- Une adresse email valable
- Un mot de passe

En cochant la case, j'accepte que mes données soient utilisées pour me faire bénéficier des services disponibles sur le Site ☐

Mentions Informatique et Libertés

Comment recueillir le consentement? Acte distinct

Article 7.2

« Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée **sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples** ».

CONDITIONS GENERALES D'UTILISATION

Article 1 Objet

Les présentes conditions définissent les conditions dans lesquelles....

(...)

Article 10 Données Personnelles

En souscrivant à notre service, l'Utilisateur accepte que ses données soient utilisées dans le cadre...

REFUSER

ACCEPTER

Données à fournir lors de la collecte

« Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable de traitement lui fournit, **au moment où les données en question sont obtenues**, toutes les informations suivantes»

(Art. 13)

Beaucoup d'informations...

1. Identité et coordonnées du responsable de traitement
2. Coordonnées du DPO
3. Finalités du traitement
4. Les destinataires des données
5. Le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers
6. La durée de conservation des données à caractère personnel ou les critères utilisés pour déterminer cette durée
7. L'existence du droit de demander au responsable du traitement l'accès aux données, la rectification ou l'effacement et la portabilité
8. Le droit d'introduire une réclamation auprès d'une autorité de contrôle
9. Des informations sur la question de savoir si l'exigence de fourniture des données a un caractère réglementaire ou contractuel et sur les conséquences éventuelles de la non-fourniture des données
10. L'existence d'une prise de décision automatisée.

Pour bénéficier de nos services, indiquez,

- Une adresse email valable
- Un mot de passe

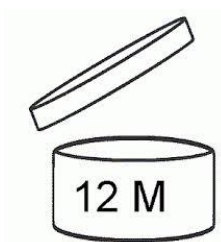
En cochant la case, j'accepte que mes données soient utilisées pour me faire bénéficier des services disponibles sur le Site ☐

Le responsable de traitement est la société JeCollecte, 3 rue des Données 75015 Paris. Elle dispose d'un Délégué à la Protection des Données qui peut être joint à DPO@jecollecte.com. Les données sont collectées exclusivement pour notre usage personnel, sauf accord exprès de l'Utilisateur. Elles nous permettent de suivre vos commandes, garantir un paiement efficace et nous assurer de votre satisfaction. Les destinataires de vos données sont exclusivement les personnes responsables du suivi et de l'exécution de vos commandes au sein de JeCollecte, à savoir, notre service logistique, marketing, financier et juridique. JeCollecte ne transfère pas de données à l'étranger sauf dans le cadre de ses échanges avec sa maison mère et les différentes filiales du groupe auquel elle appartient, pour des raisons d'amélioration de ses procédures de gestion et de suivi des commandes et des paiements notamment. Vos données sont conservées un maximum de trois mois après clôture de votre compte. Néanmoins, si aucune commande n'est enregistrée sur votre compte, JeCollecte se réserve le droit de clôturer votre compte après vous en avoir averti préalablement. Vous disposez d'un droit d'accès à vos données vous permettant à tout moment de connaître la nature des données collectées vous concernant, de demander leur rectification ou leur effacement. Ce droit s'exerce par simple envoi d'un courriel à mesdonnees@jecollecte.com. Vous pouvez également nous demander de transférer l'ensemble de vos données lorsqu'un tel transfert est possible, et conformément aux conditions mentionnées dans [nos conditions générales](#). A toute fin utile, nous vous précisons qu'en cas de difficulté en lien avec la gestion de vos données personnelles, vous avez le droit d'introduire une réclamation auprès de la CNIL ou auprès de toute autorité de contrôle compétente. Nous vous demandons accès à vos données car elles sont indispensables pour pouvoir vous livrer les biens commandés. Si vous ne remplissez pas les champs obligatoires nous ne pourrions pas traiter votre demande.

Le salut par les icônes?

« Les informations à communiquer aux personnes concernées en application des articles 13 (et 14) peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. (...) La Commission est habilitée à adopter des actes délégués aux fins de déterminer les informations à présenter sous la forme d'icônes (...) ».

(Art. 12)



signifie :
"ce produit ou cet
emballage est recyclable"



signifie :
"ce produit ou cet emballage contient
65 % de matières recyclées"



Renforcement de la protection des mineurs: création d'un régime dérogatoire pour le recueil du consentement des enfants

Article 8.2

« Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles »

Email de confirmation des parents?

L'exemple du Children's Online Privacy Protection Act

- **Providing a consent form to be signed by the parent and returned via U.S. mail, fax, or electronic scan (the “print-and-send” method);**
- **Requiring the parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;**
- **Having the parent call a toll-free telephone number staffed by trained personnel, or have the parent connect to trained personnel via video-conference; or**
- **Requesting in your initial message to the parent that the parent include a phone or fax number or mailing address in the reply message, so that you can follow up with a confirming phone call, fax or letter to the parent; or**
- **After a reasonable time delay, sending another message via the parent's online contact information to confirm consent. In this confirmatory message, you should include all the original information contained in the direct notice, inform the parent that he or she can revoke the consent, and inform the parent how to do so.**

Conformité: après la création du traitement

- Permettre à la personne concernée d'exercer ses droits (accès, effacement, limitation, portage...);
- Répondre aux demandes des autorités de contrôle...



Conformités technique et organisationnelle

Paris

Lyon

Marseille

Rennes

MERCI



www.colbert-avocats.com

h.leben@colbert-paris.com