itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Formation PME sur RGPD

PRE_Pooo_FdA-FormationRGPD_v1.1

Approche pragmatique

itrust consulting s.à r.l.
Z.I. Bombicht
L-6947 Niederanven

Tel: +352 26 176 212 6
Fax: +352 26 710 978
Web: www.itrust.lu

C. Harpes
M. Aubigny

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Introduction

Introduction

Agenda

Organisation de la formation

Approche générale

1. L'objectif du RGPD: garantir les droits de la personne concernée
2. Les piliers du RGPD: 7 Principes généraux relatifs au traitement des DCP

Pause café

Approche générale-suite (10:45-11:45)

2. Rappel : Qu'est qu'une donnée à caractère personnel (DCP)
3. Le consentement : quand est-il requis et comment doit-il être reçu ?

Collation

Et en pratique…

4. Les bons réflexes
5. Présentation des ateliers et des documents & Que faire avant d'assister aux ateliers

IL N'Y A PAS DE MAUVAISES QUESTIONS : N'HÉSITEZ PAS À INTERVENIR DURANT LES PRÉSENTATIONS

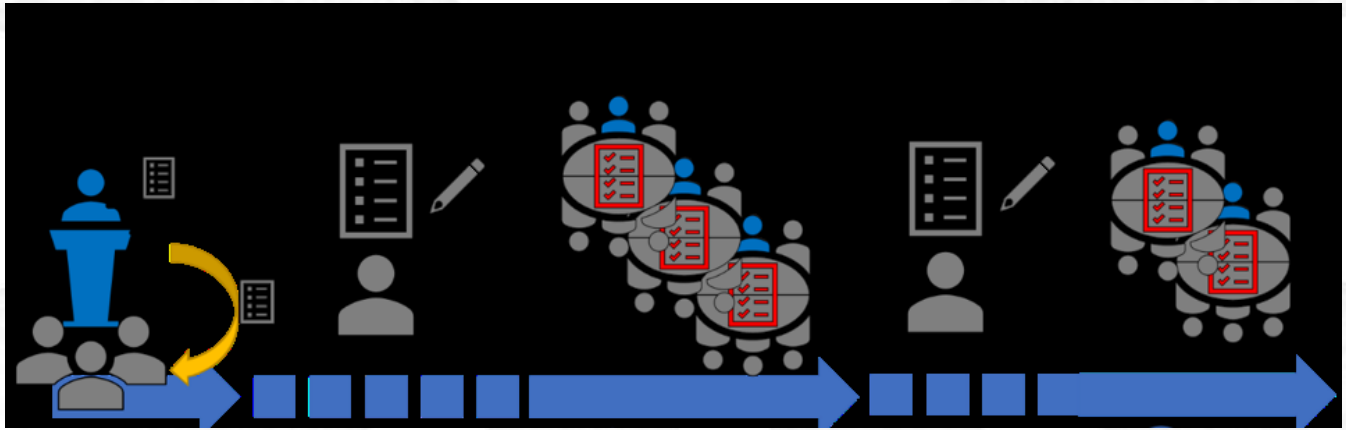
itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Organisation de la formation RGPD

L'organisation pratique des ateliers



À partir du
16 avril

Formation RGPD

Les ateliers

Registre des traitements	16/04 : 9h-11h 24/04 : 13h-15h	*Gestion et notification des violations de sécurité*
Notice de respect de la vie privée	16/04 : 11h-13h 24/04 : 15h-17h	*Gestion des sous-traitants et clauses contractuelles*
Charte de bonne conduite	23/04 : 9h-11h 25/04 : 9h-11h	*Classification des données et procédures afférentes*
Consentement	23/04 : 11h-13h 25/04 : 11h-13h	*Gestion documentaire*

L'inscription à ces ateliers est encore possible auprès des responsables de la FdA

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Approche générale du RGPD

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

1. Objectif du RGPD

1. Objectif du RGPD

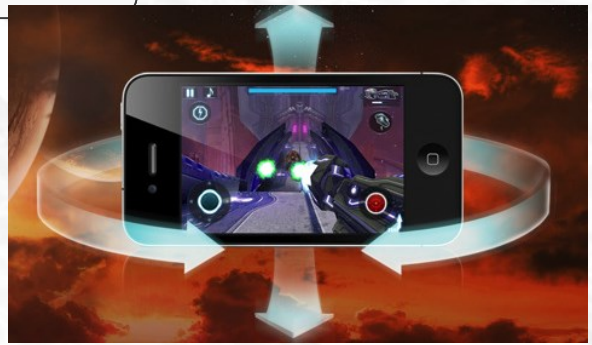
Garantir les droits de la personne

Objectif du RGPD:

« *Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.* »

Pour ce faire, les règles qui s'appliquent à tout traitement ont pour objectifs de faire respecter :

- Droit à la Transparence
- Droit de limitation du traitement
- Droit d'opposition
- Droit à l'information
- Droit à l'effacement (« droit à l'oubli »)
- Droit de Rectification
- Droit à la portabilité



1. Objectif du RGPD

Garantir les droits: rectification & effacement

Droit à la rectification: rectification ou complétion dans les meilleurs délais

Droit à l'effacement (droit à l'oubli): effacement dans les meilleurs délais si une des conditions est remplie

1. Données non nécessaires en regard des finalités du traitement
2. Consentement a été retiré
3. La personne s'oppose au traitement
4. Le traitement était illicite
5. Obligation légale
6. Collecte des DCP a été faite pour un « mineur » (<16 ans) et celui-ci veut retirer ses données après 16 ans.

Dans le cas où les données ont été rendues publiques : Effacement des données et de toutes les copies (compte tenu de la technologie et du coût)

Refus d'effacement: si liberté d'expression, obligation légale, intérêt public, archivage ou défense.

1. Objectif du RGPD

Garantir les droits: portabilité (WG Art29 16/EN/WP242)

Droit à la portabilité: droit à récupérer les données dans un format structuré **réutilisable**, droit à les transmettre à un autre responsable de traitements sous réserve des conditions suivantes

- Le traitement est fondé sur le consentement ou sur base d'un contrat
- Le traitement est fondé sur des moyens automatisés (cela ne couvre pas le traitement papier)

Note: du point de vue technique, le transfert peut être du responsable à la personne (direct download) ou d'un responsable à un autre responsable.

Quelles données ? (Art 20.1)

1. DCP de la personne concernée *(y compris les données pseudonymisées)*
2. Données produites par la personne concernée durant le traitement *(données générées ou collectées durant le traitement ou usage du service y compris les données d'analyse INDIVIDUELLE de comportement)*
3. **Restriction**: en cas de portage vers un autre responsable si les données contiennent des données à caractère personnel d'autres personnes et que leur traitement peut enfreindre leur droit.

Portage ≠ Effacement : l'usage du droit de portabilité n'est pas lié à celui de l'effacement. Le portage des données ne signifie pas l'arrêt des traitements ou de l'utilisation des services. Le responsable peut conserver et traiter les données jusqu'à l'échéance sauf demande explicite d'effacement. De même le portage des données n'est pas un motif de suspension du service.

1. Objectif du RGPD

Garantir les droits: portabilité (WG Art29 16/EN/WP242)

Règles gouvernant le droit à la portabilité :

1. Obligation pour le responsable d'informer la personne concernée de ce droit (art 13.2.b & 14.2.c).
   Bonne pratique: informer la personne concernée de ce droit avant la fermeture définitive de son compte
2. Identification de la personne concernée avant la réponse à la requête: pas de règle formelle dans le RGPD bien au contraire puisque obligation de répondre. Cependant, le responsable, **en cas de doute,** peut demander des informations supplémentaires pour identifier l'auteur de la requête comme la personne concernée.
3. Temps de réponse à la requête: délais raisonnables (<1 mois après réception) que ce soit pour répondre positivement ou négativement

Refus/Paiement/Délais:

1. Refus ou paiement: possible seulement dans le cas de demandes injustifiées et répétitives.
2. Délais : dans le cas où la masse de données dépasserait la capacité normale de transmission, un délai peut être accordé pour utiliser un moyen plus adapté (gravure CD/DVD, etc.). Délais maxi: 3 mois

1. Objectif du RGPD

Garantir les droits: portabilité (WG Art29 16/EN/WP242)

Remise des données : le comment du processus

1. Format: le format doit permettre une réutilisation. (art 20.1); format structuré lisible par une machine. Le point crucial est interopérabilité des solutions et non leur comptabilité.
2. Metadata: le responsable doit fournir autant de méta data que nécessaires et selon une granularité suffisante pour la réutilisation *(portage des emails en format PDF ne suffit pas)*
3. Cas des collections importantes ou complexes: pas de réponse dans RGPD cependant les informations fournies par le responsable du traitement doivent être suffisante pour que la personne concernée puisse réutiliser ses données.
4. Sécurisation des données lors et après leur transfert:
   a) S'assurer que les données parviennent réellement à la personne sans risque d'interception.
   b) Informer la personne concernée de la nécessité de protéger ses informations
      Bonne Pratique: Fournir les données dans conteneur chiffré

Note: Une solution pour répondre à l'obligation de portabilité peut être de mettre en place une API sécurisée et documentée.

1. Objectif du RGPD

Garantir les droits: opposition (WG Art29 16/EN/WP242)

Droit d'opposition: droit à s'opposer à tout moment à un traitement fondé sur art 6.1.e ou art 6.1.f sous réserve des conditions suivantes

- Pour des raisons tenants à la situation particulière de la personne concernée
- Le traitement à des fins de prospections (y compris le profilage)

Le responsable des traitements peut refuser

- si motifs légitimes et impérieux prévalant sur les intérêts et les droits de la personne
- si exercice ou défense de droits en justice
- si (dans le cas d'un traitement pour recherche scientifique ou historique ou traitement statistique) le traitement repose sur une mission d'intérêt public.

Obligation du responsable des traitements : Information sur le droit d'opposition

NB: Droit d'opposition peut être exercé à l'aide de procédé automatique sous réserve du respect de la directive ePD

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

2. Les 7 piliers du RGPD: atteindre l'objectif

2. Les 7 piliers du RGPD

Principes généraux concernant le traitement des DCP

7 grands principes à respecter lors de la mise en œuvre d'un traitement (cf. art. 5)

- Licéité/Loyauté/Transparence
- Limitation de la finalité
- Minimisation des données
- Exactitude
- Conservation (limitation)
- Intégrité et confidentialité
- Responsabilité

2. Les 7 piliers du RGPD

Pilier 1: Licéité, Transparence et loyauté

Le traitement des données en général est licite si sa base légale est l'une de celles-ci:

1. Fondé sur consentement
2. Fondé sur un contrat
3. Fondé sur obligation(s) légale(s)
4. Fondé sur un intérêt vital
5. Fondé sur une mission d'intérêt public
6. Fondé sur des intérêts légitimes (*balancing of interests*)

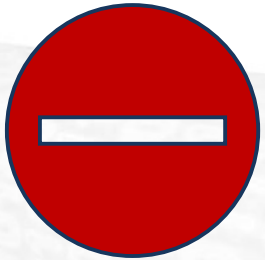
N. B. Habituellement, un traitement est fondé sur une seule base légale, mais il se peut aussi que plusieurs puissent être invoquées en raison du type de données traitées.

2. Les 7 piliers du RGPD

Pilier 1: Licéité, Transparence et loyauté

Le traitement des données sensibles (cf. p. 34) est **INTERDIT** sauf si la base légale du traitement est l'une de celles-ci: (art 9)

1. fondé sur un consentement explicite
2. dans le cadre du droit du travail, de la sécurité sociale ou de la protection sociale
3. pour la sauvegarde des intérêts vitaux de la personne
4. pour un organisme à but non lucratif
5. **manifestement** rendues publique
6. dans le cadre de la défense d'un droit en justice
7. fondé sur des raisons médicales ou associées
8. pour des raisons de santé publique
9. pour archivage, recherche ou statistique
10. dans le cadre d'un législation « nationale » notamment en matière de données génétiques, biométriques, etc.



NB: Pour le point 10 la législation nationale peut autant permettre que restreindre les traitements des données dites sensibles

2. Les 7 piliers du RGPD

Pilier 1: Licéité, Transparence et loyauté

Le traitement des données relatives aux condamnations et aux infractions uniquement sous le contrôle de l'autorité publique (art 10) ou si explicitement autorisé par autorité nationale.

Des situations particulières sont encadrées par le RGPD: traitement

1. à des fins journalistiques, ou expressions universitaires, artistiques ou littéraires (art 85)
2. pour des données incluses dans les documents officiels (art 86)
3. pour les données d'identification nationale (art 87)
4. pour des fins d'archivage d'intérêt public ou de recherche scientifique, historique ou statistique (art. 88)
5. Fondé sur Directive ePD (ePrivacy Directive): (en révision -25 mai)
   a) cookies
   b) Traffic data
   c) Donnée de localisation
   d) Marketing direct
6. Pour les données relatives aux enfants (<16 ans)

2. Les 7 piliers du RGPD

Pilier 1: Licéité, Transparence et loyauté

Le traitement et les informations sur le traitement doivent assurer:

1. Facilité de l'accessibilité
2. Facilité de compréhension
3. Terminologie claire et simple
4. Identité du responsable du traitement
5. Sur la/les finalités du traitement
6. Droit d'obtenir confirmation et communication des DCP traitées
7. Sur les risques, règles, garanties et droits liés au traitement
8. Sur les modalités d'exercices de leurs droits
9. Opérations sont-elles enregistrées pour éviter tout abus

2. Les 7 piliers du RGPD

Pilier 1: Licéité, Transparence et loyauté

Le groupe de travail Article 29 (Article 29 Data Protection Working Party) a donné des lignes directrices pour assurer la transparence des traitements (17/EN WP260):

« *Le principe de transparence requiert que toute information et communication relatives au traitement des données à caractère personnel doivent être facilement accessibles et facilement compréhensibles, et doivent être exprimées dans un langage clair et simple* » REC. 39

Art 12:

1. Concise, transparent, intelligible et facile d'accès (12.1)
2. En langage clair et simple (12.1)
3. Attention particulière aux enfants (12.1)
4. Écrit (12.1)
5. Oral (12.1)
6. Gratuitement (12.5)

2. Les 7 piliers du RGPD

Pilier 1: Licéité, Transparence et loyauté

1. Concise, transparent: clairement séparé des autres conditions du traitement (notice, charte, politique)…
2. Intelligible: doit être compréhensible pour un lecteur moyen (AUDIENCE)
3. Facilement accessible: la personne concernée ne doit pas à avoi chercher
4. Langage clair et simple signifie information exprimée en un lan évitant une syntaxe complexe (longues phrases avec subordonn sans abstraction ou ambivalence des termes (pas d'interprétati possible).

Quelques règles:

a) Éviter les expressions comme « il se peut », « il se pourrait », « quelques », « possible »
b) Utiliser la voix active et non passive
c) Pas de vocabulaire légal, technique ou appartenant à un domaine spécifique
d) Si plusieurs langues : vérifier la cohérence dans les autres langues (éviter la translittération)

2. Les 7 piliers du RGPD

Pilier 2: Limitation de la finalité

Finalité au moment de la collecte

1. Finalité(s) spécifique(s)
2. Finalité(s) explicite(s)
3. Finalité(s) légitime(s)
4. Finalité(s) documentée(s)

Finalités secondaires (après la collecte): Finalité(s) différente(s) (Information sur ces finalités avant tout traitement)

Finalité(s) compatibles par principe avec la (les) finalité(s) initiale(s) c'est-à-dire :

1. À des fins d'archivage d'intérêt public ou de recherche scientifique, historique ou statistique
2. Fondé sur consentement initial
3. Fondé sur obligation légale

Si finalité(s) non compatible(s) : la compatibilité entre-finalités présumées fondée su

1. un lien avec la (les) finalité(s) initiale(s)
2. les rapports spécifiques entre la personne concernée et le responsable du traitement
3. la nature des données
4. un lien de causalité entre les traitements
5. l'existence de mesure de sécurité comme le chiffrement et la pseudonymisation

Pilier 2: Limitation de la finalité

Le principe de limitation du traitement des données à caractère personnel oblige autant le responsable que le processeur ainsi que pour le fournisseur de solution IT à mettre en place des mesures pour limiter usage des DCP pour une autre finalité

Pour le responsable du traitement/processeur

1. Mesures spécifiques ou de minimisation pour éviter ou rendre difficile l'usage des données pour une autre finalité
2. Si DCP utilisée pour des finalités spécifiques, est-ce que la gestion d'accès à ces DCP prévient ou rend difficile l'utilisation de ces DCP pour une autre finalité

Pour le fournisseur de solution IT (service, software ou système)

1. Design de la solution permettant d'éviter tout usage des DCP hors finalité
2. Information et code de bonne conduite pour favoriser l'application du principe de limitation par l'utilisateur (pour le sous-traitant)

2. Les 7 piliers du RGPD

Pilier 3: Minimisation des données

Les traitements doivent utiliser le minimum de données à caractère personnel c'est-à-dire en respectant les principes suivants lors du choix des DCP à collecter:

1. Adéquates/finalité(s): par ex. en évitant les données superflues.
2. Pertinentes/finalités (s): par ex. en évitant une précision inutile.
3. Limités/finalité(s) :notamment en ce qui concerne la durée de rétention (minimale).
4. Utilisation de technique de minimisation comme anonymisation ou pseudonymisation
5. Design des processus permettant de

≠

2. Les 7 piliers du RGPD

Pilier 4: Exactitude

Les données à caractère personnel doivent être maintenues exactes :

Pour le responsable du traitement/processueur

1. Vérification que les DCP sont exactes et à jour
2. Processus rapide de correction ou de destruction des DCP non exactes

Pour le fournisseur de solution IT (service, software ou système)

1. Design des processus permettant d'assurer l'exactitude des DCP
2. Fonctionnalités du processus de traitement permettant d'assurer la rectification ou effacement des DCP erronées.
3. Fonctionnalités du processus de traitement permettant d'assurer l'exactitude des DCP.
4. Information et code de bonne conduite pour favoriser l'application du principe de limitation des DCP par utilisateur

2. Les 7 piliers du RGPD

Pilier 5: Conservation

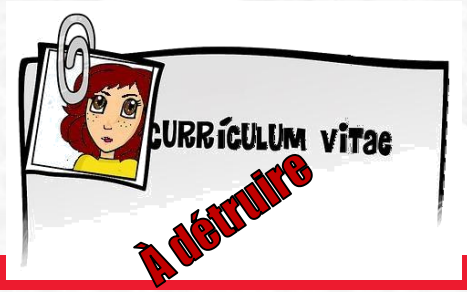
Les données à caractère personnel doivent être conservées uniquement lorsqu'elles sont nécessaires à la finalité du traitement:

Pour le responsable du traitement

1. Traitement rendant impossible l'identification de la personne physique au-delà des finalités du traitement
2. Sinon traitement à de seules fins d'archivage d'intérêt public ou de recherche scientifique, historique ou statistique

Pour le processeur

1. Design des processus permettant d'assurer la limitation du stockage des DCP
2. Fonctionnalités du processus de traitement permettant d'assurer la limitation du stockage des DCP.
3. Information et code de bonne conduite pour favoriser l'application du principe de limitation du stockage des DCP par utilisat



2. Les 7 piliers du RGPD

Pilier 6: Confidentialité et intégrité des données

Les données à caractère personnel doivent être maintenues confidentielles et intègres

Pour le responsable du traitement ou le processeur

Les mesures de sécurité (techniques et organisationnelles) appliquées au traitement sont suffisantes pour assurer une protection des DCP contre

1. un usage non autorisé ou illégal,
2. une destruction ou une corruption.

Pour le fournisseur de solution IT (service, software ou système)

Il a les éléments suivants

1. Design des processus,
2. fonctionnalités,
3. Information et code de bonne conduite

afin d'assurer le maintien de la confidentialité et de l'intégrité des DCP.

2. Les 7 piliers du RGPD

Pilier 7: Responsabilité

Le responsable du traitement (et médiatement le processeur) doit pouvoir rendre compte du respect du RGPD (notamment en cas d'incident).

Pour le responsable du traitement

1. Mettre en œuvre des mesures de sécurité (techniques et organisation
   pour démontrer la conformité du traitement aux grands principes du R
2. Les mesures de sécurité (techniques et organisationnelles) sont revue
   à jour régulièrement (efficacité).

Pour le fournisseur de solution IT (service, software ou système)

1. Design des processus permet de démontrer la conformité du traiteme
   grands principes du RGPD.
2. Fonctionnalités du processus de traitement permet de démontrer la c
   du traitement aux grands principes du RGPD.
3. Information et code de bonne conduite pour que l'usage du traitement
   permette d'assurer ce devoir de responsabilité

itrust consulting

FEDERATION DES ARTISANS

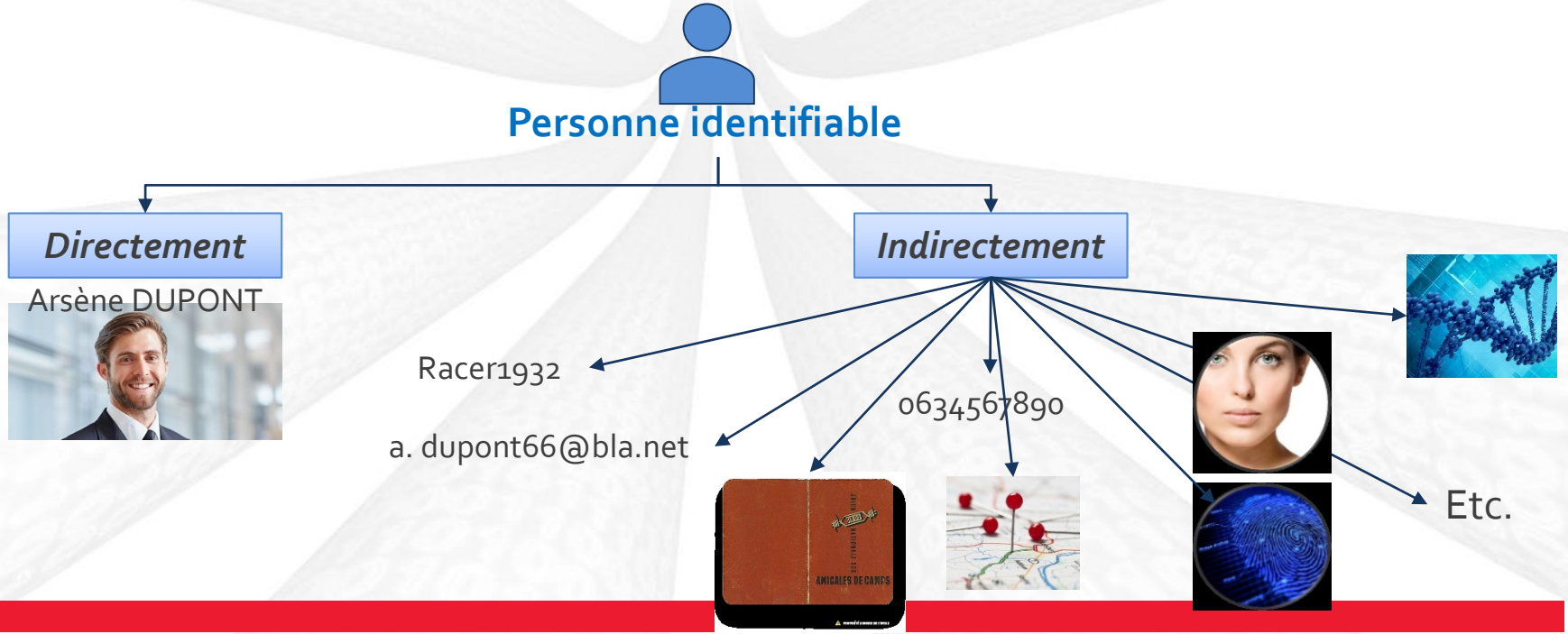
Move securely within the cyberworld

Données à caractère personnel (DCP): petit rappel

Terminologie: donnée à caractère personnel

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

Article 4: *« données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable.*

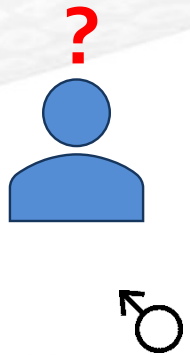


Terminologie: donnée à caractère personnel

Cas pratique : Identifier une donnée à caractère personnel

Toutes ces données sont caractéristiques d'une personne physique…

- Année de naissance: 1966
- Date et lieu de naissance: 23/06/2008 + Luxembourg
- Date lieu de naissance et sexe: 14/05/2010 + Clervaux +
- Heure, date, lieu de naissance et sexe: 23/06/2008 + Luxembourg + 02:40
- Localisation aléatoire/régulière
- Mac adresse



… pourtant tout n'identifie pas la personne physique

Terminologie: donnée à caractère personnel

Catégorie de données à caractère personnel

Données générales

- Informations sur la personne physique : Nom, prénom corrélé au numéro de téléphone, état civil, identité, données d'identification, adresse email, etc. Vie personnelle (habitudes de vie, hobbies, situation familiale, etc.)
- Identification de la personne morale si elle permet d'identifier une personne physique
- Informations sur l'activité professionnelle: Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.), Informations sur ses conditions de travail, etc.
- Temps de travail (début/fin/pause) en relation avec la personne physique
- Empreintes numériques
- L'image d'une personne enregistrée par une caméra
- Adresse IP dynamique
- Cookies lorsqu'il contient un identifiant unique de la personne physique
- Informations de localisation (déplacements, données GPS, GSM, etc.) de la personne physique
- Données de localisation IP (Wi-Fi corrélé avec l'adresse Mac unique)
- Données de connexion (adresse IP, logs, etc.)
- Information RFID si elle permet d'identifier la personne physique de manière unique

Catégorie de données à caractère personnel

Données sensibles (Art 9.1)

- Origine ethnique ou raciale
- Opinions politiques
- Croyances philosophiques ou religieuses
- Appartenance syndicale
- Informations génétiques
- Données biométriques utilisées pour identifier d'une manière unique une personne physique
- Informations sur des données de santé
- Information sur la vie sexuelle ou les orientations sexuelles

Données personnelles relatives aux condamnations pénales et aux infractions (art. 10)

- Données enregistrées sur des infractions
- Casier judiciaire

Terminologie: donnée à caractère personnel

Catégorie de données (classification CNPD)

Dans son outil, la CNPD fait référence à la classification des données suivante

À: Données d'identification
B: Données bancaires et financières autres que celles sujettes aux traitements concernant le crédit et la solvabilité des personnes
C: Caractéristiques personnelles autres que celles sujettes aux traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données relatives à la santé et à la vie sexuelle, y compris le traitement des données génétiques
D:Données physiques
E: Habitudes de vie et de consommation autres que celles sujettes aux traitements relatifs à la vie sexuelle
F: Données psychiques autres que celles sujettes aux traitements relatifs à la santé
G: Composition du ménage
H: Loisirs et intérêts
I: Affiliations et situation de membres
K: Biens et services fournis et reçus
L: Caractéristiques du logement
M: Données relatives à la santé pour les traitements mis en œuvre par les établissements hospitaliers et les médecins traitants et ceux nécessaires à la sauvegarde des intérêts vitaux d'une personne incapable de donner son consentement (art.6 et 7 de la loi)
N: Éducation, formation et qualification
O: Profession et emploi – Salaire – Évaluation - Sécurité
P: Données judiciaires sujettes aux traitements visés à l'article 8 de la loi
Q: Données raciales ou ethniques sujettes aux traitements visés à l'article 6 paragraphe 2 lettre (c) de la loi Q.
R: Données relatives au comportement sexuel sujettes aux traitements visés à l'article 6 paragraphe 2 lettre (c) de la loi
S: Opinions politiques aux traitements visés à l'article 6 paragraphe 2 lettre (d) de la loi
T: Affiliation syndicale sujette aux traitements visés à l'article 6 paragraphe 2 lettre (d) de la loi
U : Convictions philosophiques ou religieuses sujettes aux traitements visés à l'article 6 paragraphe 2 lettre (d) de la loi
V: Enregistrement d'images
W: Enregistrements de sons

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

3. Consentement

3. Consentement

Quand a-t-on besoin du consentement ?

Quand n'a-t-on pas besoin d'un consentement pour effectuer le traitement ?

Chaque fois que le traitement est fondé sur une autre raison légale, soit:

Performance d'un contrat

Sauvegarde des intérêts vitaux

Obligation légale

Intérêt public

Intérêt légitime (*balancing of interests*)

3. Consentement
Définition

Art 4.11 « *consentement de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »

Donné librement

Indication non ambiguë
cceptation

Spécifique

Informé

3. Consentement

Libre : commentaire WG Art29: 17/EN/259

Libre/donné librement: implique un choix réel et sous le contrôle du sujet

1. Le choix ne doit être en aucun cas contraint par le processeur (notamment dan le cas d'une relation déséquilibrée).
2. Dans le cas de la délivrance d'un service, le consentement ne doit couvrir que les données strictement nécessaires à la réalisation du contrat.
3. Dans le cas d'un contrat : il est important d'évaluer le périmètre du contrat même si dans ce cas le consentement est implicite au contrat.

Un contrat ne peut en aucun cas être la base légale de traitement de données sensibles

3. Consentement

Libre: commentaire WG Art29: 17/EN/259

Libre/donné librement:

4. Le consentement ne doit pas être donné en général, mais pour chaque traitement en particulier (càd en relation avec sa finalité propre).
5. Le processeur doit pouvoir prouver que le consentement peut être refusé à tout moment sans préjudice financier.

3. Consentement

Spécifique: commentaire WG Art29: 17/EN/259

Spécifique/finalité(s): faire preuve de clarté

1. Spécifier les finalités.
2. Assurer la possibilité d'un consentement granulaire
3. Assurer la séparation entre les informations qui regardent le consentement au traitement et les autres informations (contractuelles notamment)

3. Consentement

Informé: commentaire WG Art29: 17/EN/259

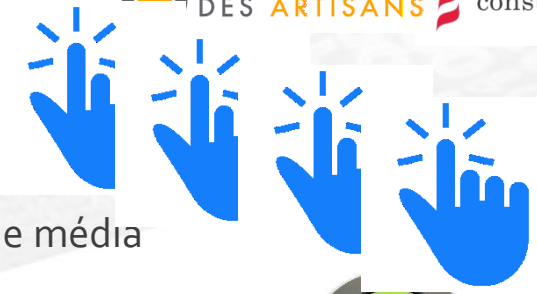
Informé: le consentement doit être fait sur une base réelle de connaissance de la part de l'utilisateur: dans le cas contraire pas de consentement.

Spécification minimale de l'information.

a) Identité du responsable du traitement
b) Finalité de chaque opération de traitement
c) Type de données collectées
d) Existence d'un droit au retrait du consentement
e) Information si décisions automatisées
f) Information si le consentement inclut celui du transfert de données dans un pays tiers.

3. Consentement

Non ambigu: commentaire WG Art29: 17/EN/259



Informé:

1. Moyen de transmettre l'information: pas d'obligation de type de média
2. Accent sur la compréhension de l'acte de consentement

Non ambigu:

1. L'acte de consentement doit être formalisé dans un processus actif: action délibérée (l'utilisation de case pré cochée est interdite).
2. Dans le cas de système électronique : l'action peut être un geste physique.
3. Le processus de consentement doit éviter tout phénomène de fatigue ou lassitude de la part de l'utilisateur

3. Consentement

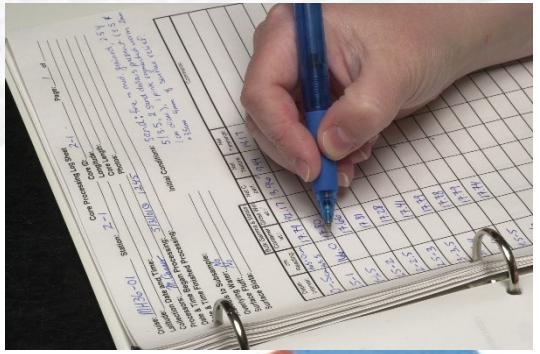
Explicite : commentaire WG Art29: 17/EN/259

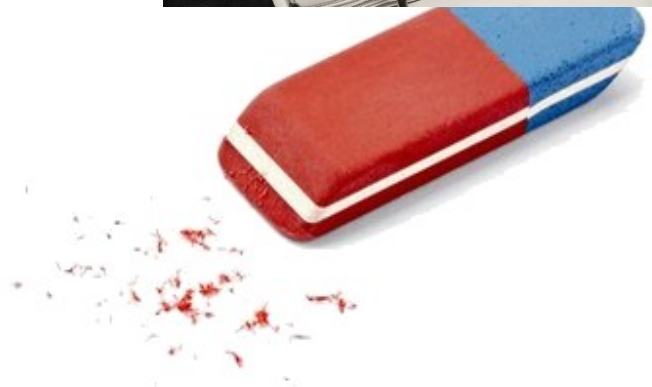
Consentement explicite: dans certains cas (**données sensibles**)

1. Utilisateur donne une déclaration formelle (par exemple écrite).
2. Ce qui ne veut pas dire papier : formulaire électronique, email ou processus à deux étapes (réponse requise avec mention « Je suis d'accord ».)

Conditions supplémentaires de validité:

1. Obligation pour le responsable de démontrer que l'utilisate
2. Obligation d'assurer un moyen de revenir sur son consente
3. Note : Limitation dans le temps: pas de limitation a priori sauf si changement d
   Bonne pratique: demander à intervalle régulier.





3. Consentement

Consentement & information et sollicitation commerciales

1. Obligation de recueillir le consentement avant tout traitement (OPT-IN) pour
    1. sollicitation par voie électronique (sms, mail, mms)
    2. céder ou échanger les coordonnées électroniques à cette fin
2. Exceptions:
    1. Envoi sur adresse professionnelle et objet en rapport avec le business
    2. Message pour produit ou service identiques
3. Obligation à respecter:
    1. le droit de s'opposer (de manière simple et gratuite)
    2. Limitation de la conservation des données (p.ex. <3 ans sans réponse de l'intéressé)
    3. Assurer l'impossibilité d'utiliser les données pour d'autres fins (clause contractuel en cas d'utilisation d'un prestataire de service)
4. Interdiction:
    1. Collecter information sur des sites ou des forum
    2. Présumé du consentement (coche préremplie)
    3. Conditionner l'accès à un service à l'acceptation de la sollicitation.
5. Utilisation des annuaires commerciaux publics : possible

3. Consentement
Comment faire ?

1. Aucune règle sur le média utilisé pour informer:
   - De manière écrite ou orale
   - Papier, électronique
   - Message audio, vidéo, etc.
2. Le plus important: **recueillir** une indication non ambiguë du choix: **action clai**
   affirmative et non lié à l'acceptation d'un contrat ou des termes et conditions
   service, etc.
3. **Enregistrer** une preuve de ce consentement.

Pratiquement:

- Collecter des réponses formelles (par exemple à l'acceptation d'une notice de resp
  privée): lettre, email de réponse à une demande formelle
- Collecter l'acceptation via un formulaire (non ambigu quant à l'information)

3. Consentement

Consentement déjà reçu sous Dir 95/46/EC

Les traitements en cours licites et fondés sur le consentement ne requièrent pas automatiquement de recueillir à nouveau le consentement de la personne concernée.

Cependant: le responsable du traitement doit vérifier que le consentement déjà recueilli est conforme au RGPD c'est-à-dire:

- Une trace du consentement a été conservé
- Il existe une procédure d'annulation du consentement conforme (y compris au niveau de la granularité)
- L'information était correctement donnée (claire, précise, etc.)

Et si le consentement n'est pas conforme, avant le 25 mai:

1. Demandez à nouveau le consentement,
2. Évaluez si le traitement peut être fondé sur une autre base légale, ou
3. Arrêtez le traitement

itrust consulting

Move securely within the cyberworld

FEDERATION DES ARTISANS

4. Les bons réflexes pour atteindre la conformité

4. Les bons réflexes pour atteindre la conformité

Les points essentiels à considérer

- Faire **l'inventaire** des activités de traitements et de leur finalité principale (et secondaire) ainsi que la licéité de chaque traitement
- Pour chaque traitement, identifier le **responsable** (contrôleur) et le cas échéa **traitant**s (processeur) et le DPO.
- Déterminer le **type de chaque donnée** traitée et vérifier qu'elles sont utilisées à en lien avec la finalité et de manière adéquate (minimisation)
- Vérifier que pour chaque donnée (ou groupe de données) une **date de rétention** et qu'un processus de destruction sécurisé est en place
- Vérifier que des **mesures de sécurité** ont été définies pour assurer la protection d le suivi de leur accès et le contrôle de ces mesures (application/efficience)
- Identifier les **partages de données** (interne/externe) pour éviter toute violation que ce partage de données est possible (légaux et assurant la protection)

4. Les bons réflexes pour atteindre la conformité

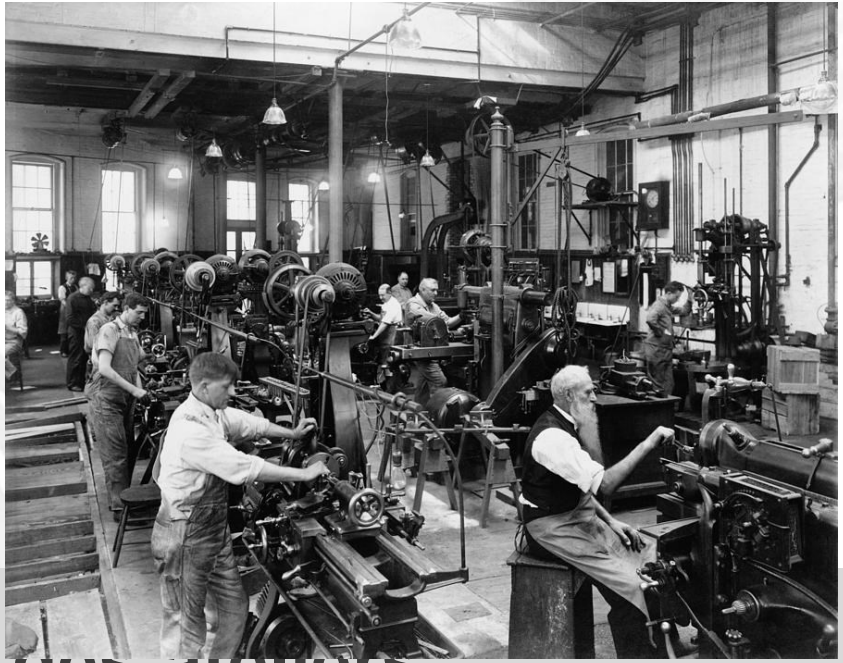
Les documents à rédiger

- Registre des traitements (obligatoire): remplace la notification à la CNPD pour de nombreux traitements
- Déclaration(s) de respect de la vie privée : à destination interne et externe
- Charte d'utilisation des systèmes d'information/Code de bonne conduite
- Clause contractuelle dans les contrats des sous-traitants pour assurer un respect du RGPD lors des traitements
- Procédure de gestion des incidents et de notification des violations
- Procédure de portage des données
- Procédure de surveillance et de contrôle de la sécurité associée à la protection des données à caractère personnel
- Analyse d'impact (si risque élevé)

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld



5. Présentation des ateliers

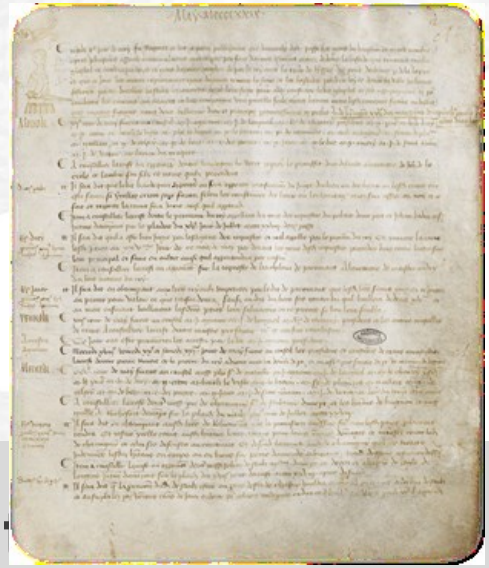
Plan de la présentation de chaque atelier

1. Remise en perspective par rapport aux demandes du RGPD
2. Présentation des documents
3. Que faire avant l'atelier ?
4. Que ferons-nous pendant l'atelier ?

itrust consulting

Move securely within the cyberworld

FEDERATION DES ARTISANS



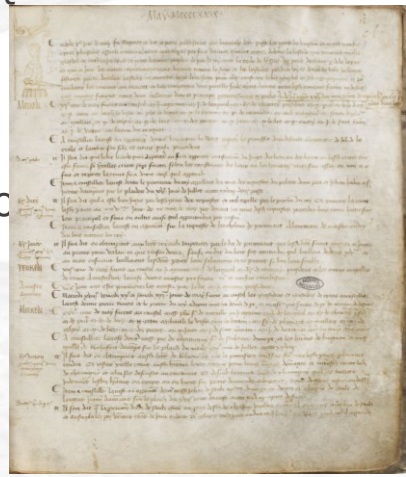
5.1 Registre des traitemen

5.1. Registre des traitements

Conditions d'établissement

L'établissement d'un registre des traitements et une obligation pour le responsable des traitements et pour les sous-traitants du traitement (Art. 30-1 et 30-2).

Il remplace les anciennes notifications des traitements à la CNPD



Exception: Ne s'applique pas aux organisations de moins de 250 employés SAUF SI l'une des conditions suivantes est remplie:

1. Risque pour les droits et libertés des personnes
2. Non occasionnel
3. DCP sensible (art 9 et 10)

Pratiquement: il est conseillé d'établir ce registre dans tous les cas et surtout de prendre en compte tous les traitements (électronique/papier)

5.1. Registre des traitements

Contenu

Que doit contenir à minima un registre (pour le responsable du traitement)

a) Nom et coordonnées du responsable du traitement. (possiblement nom du responsable conjoint et du DPD)
b) Finalité du traitement
c) Description catégorie de données
d) Catégorie des destinataires
e) Transfert des données vers pays tiers et organisation internationale
f) Dans la mesure du possible: Délais prévus pour effacement des DCP
g) Dans la mesure du possible: Description générale des mesures de sécurité

Que doit contenir à minima un registre (pour le sous-traitant du traitement)

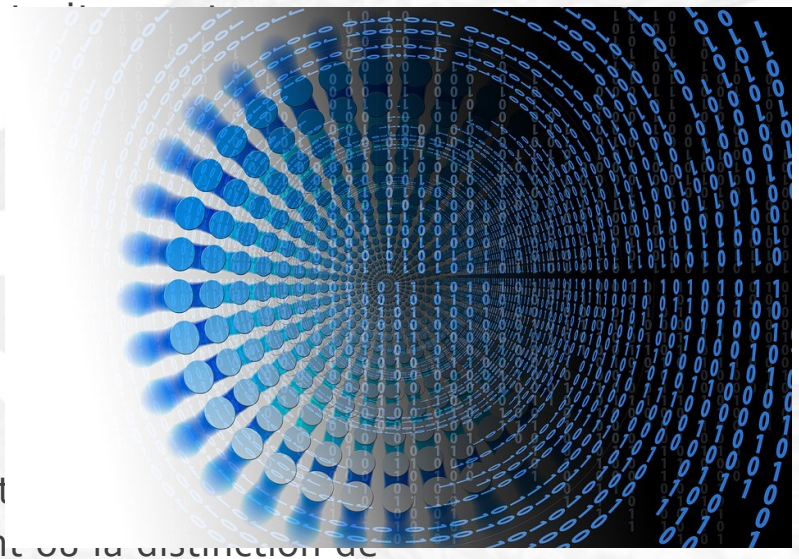
a) Nom et coordonnées du sous-traitant du traitement et de chaque responsable du traitement pour lequel le sous-traitant agit. (possiblement nom du responsable conjoint et du DPD)
b) Description catégorie de données
c) Transfert des données vers pays tiers et organisation internationale
d) Dans la mesure du possible: Description générale des mesures de sécurité

5.1. Registre des traitements

Traitements à renseigner

Traitement typique à renseigner dans un registre des

- Gestion des dossiers du personnel et CV candidature
- PayRoll
- Gestion des factures et des offres clients, fournisseurs
- Gestion de l'utilisation des moyens IT par le personnel
- Gestion de la géolocalisation des employés
- Gestion des bases de données prospects, etc.



Pratiquement : il appartient au responsable du traitement
et le type de traitement en s'assurant que le regroupement
processus est logique.

5.1. Registre des traitements

Un modèle

Modèle de registre de traitement (modèle Excell) permettant d'encoder l'ensemble des traitements. Ce document comprend diverses feuilles:

- Historique : pour indiquer comment le document est géré (groupe de travail distribution, approbation..)
- Structure : information sur la structure
- Entités: Information générale sur les traitements ainsi que sur les responsabilités au sein de l'organisation quant à la protection des données à caractère personnel (DCP)
- Synthèse: Résumé des informations importantes de chaque traitement
- Registre: Information sur les divers traitements selon la RGPD
- Opt: Mesure gén.: En option, Check-list des mesures de sécurité mises en place pour l'ensemble des traitements afin de garantir la protection des DCP.
- Opt: Risques max.: Tableau permettant d'indiquer les niveaux du risque le plus élevés de chaque traitement.
- Licéité et Échelles : Tableaux d'information sur les bases légales de licéité et échelles utilisées dans l'analyse de risque.

Le modèle fourni est prérempli pour quelques traitements types (de manière générique).

5.1. Registre des traitements

Organisation pratique de l'atelier

Que faire avant l'atelier « Registre des traitements »

- Adapter à votre entreprise les traitements déjà préremplis
- Identifier si d'autres traitements existent au sein de votre entreprise
- Encoder ces nouveaux traitements
- Noter l'ensemble des questions qui se poseraient et nous les transmettre (RGPD@itrust.lu)

Que ferons-nous pendant l'atelier « Registre des traitements »

- Nous traiterons (de manière anonymiser) l'ensemble des questions reçues pour vous aider à finaliser vos registres en
  - replaçant la question dans le cadre de la réglementation
  - en proposant une ou plusieurs solutions.
- Nous vous proposerons de vous guider dans l'encodage individuel de vos traitements (accompagnement au cas par cas) durant l'atelier.
- Nous répondrons aux questions supplémentaires ou initierons des réflexions en fonctions des exemples.

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

5.2. Notice de respect de la vie privée

5.2. Notice de respect de la vie privée

Généralités

Le responsable doit permettre aux personnes concernées d'exercer leurs droits et notamment le premier celui d'être informé. **(pas de guide officielle)**

Comment informer les personnes concernées ? Généralement au moment de la collecte. Mais cela dépend de la manière dont on collecte les données.

Sous quelles formes: Pour remplir toutes les obligations de RGPD en matière d'information il est souvent utile d'établir une notice de respect de la vie privée, ou engagement de confidentialité (*privacy notice*, *privacy policy* etc.)

- Modèle long (à rédiger en premier)
- Modèle court (avec référence au modèle long) reprenant les éléments clés du modèle long. Ce modèle pourra notamment servir lors du recueil de consentement.

Quand revoir les notices ? Dès que les modalités du traitement changent: nouvelles finalités, nouveaux sous-traitants, changement majeur (transfert, profilage)

5.2. Notice de respect de la vie privée

Contenu

Une notice de respect de la vie privée doit cibler un groupe de destinataire et contenir en général les éléments suivants

- Déclaration de principe rappelant que l'organisation prend en considération les personnes et leur droit en matière de traitement des données à caractère personnel
- Règles de conduite quant au traitement (avec la date de dernière mise à jour)
  - Engagement de la société
  - Périmètre de ces règles (finalité(s) des traitements y compris secondaire(s))
  - Responsabilité (responsable du traitement, DPD) avec coordonnées
  - La mise en œuvre du consentement
  - Quelles données et comment les données sont collectées
  - Comment les données personnelles sont utilisées
  - Qui sont les destinataires des données (partage et communication)
  - Transfert des données
  - Protection des données
  - Quels sont les droits des personnes et comment les exercer
  - Les modalités de changement de ces règles

Possiblement

- Utilisation spécifique des données
  - Cookie (site web)
  - Service Google Analytics
  - À des fins commerciales

5.2. Notice de respect de la vie privée

Modèle

Modèle de Notice: pour l'atelier notice de respect de la vie privée, vous disposerez de 3 documents

1. Un guide de rédaction
2. Un modèle de notice à destination de vos employés
3. Un modèle long de notice à destination vos clients, sous-traitants, visiteurs de site web…

5.2. Notice de respect de la vie privée

Organisation pratique de l'atelier

Que faire avant l'atelier « Notice de respect de la vie privée »

- Adapter ou rédiger pour votre entreprise le ou les notices
- Noter l'ensemble des questions qui se poseraient et nous les transmettre (RGPD@itrust.lu)

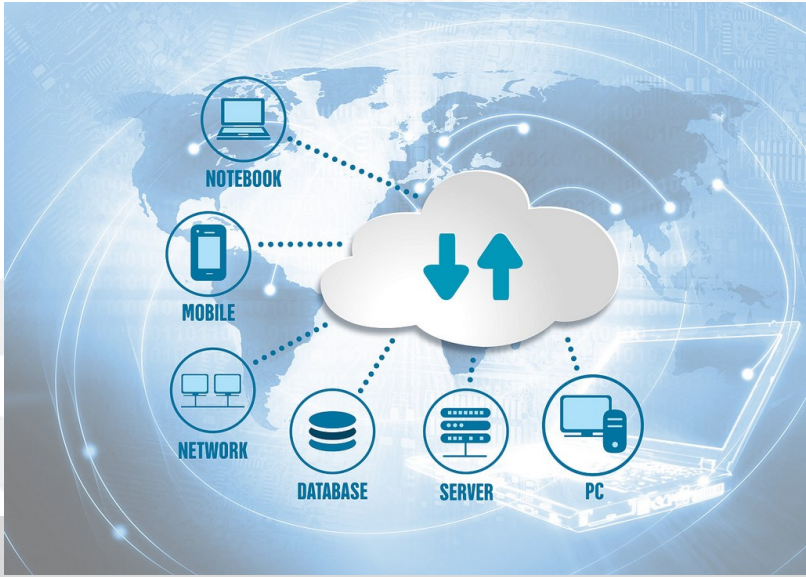
Que ferons-nous pendant l'atelier « Notice »

- Nous traiterons l'ensemble des questions reçues pour vous aider à finaliser vos registres en
  - replaçant la question dans le cadre de la réglementation
  - en proposant une ou plusieurs solutions
- Nous vous proposerons de vous guider dans l'encodage individuel de vos notices (accompagnement au cas par cas) durant l'atelier
- Nous répondrons aux questions supplémentaires ou initierons des réflexions en fonctions des exemples

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld



5.3. Charte de bonne conduite en sécurité de l'information

5.3. Charte de bonne conduite

Principes

Les grands principes de sécurité dans le RGPD:

- **Obligation de rendre des comptes**

Art 24.1 « *Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre* ***des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement.*** *Ces mesures sont réexaminées et actualisées si nécessaire.* »

- **Obligation de mettre en œuvre des mesures de manière logique et ciblée**

Art 32.1 « ***Compte tenu de l'état des connaissances, des coûts de mise en œuvre*** *et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre* ***les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque… »***

Art 32.2 « *Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la* ***destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.*** »

5.3. Charte de bonne conduite

But et contenu

Une manière simple d'organiser la sécurité est de mettre en œuvre une charte de bonne conduite en matière de sécurité de l'information.

But de la Charte:

- Informer tout utilisateur de ses rôles et responsabilités lorsqu'il utilise les systèmes informatiques (et les informations) de sa société notamment en ce qui concerne sa responsabilité en matière de protection des données.
- Avoir leur consentement

Contenu:

1. Principes de protection des données à caractère personnel
2. Code de déontologie propre à l'entreprise
3. L'importance de chacun dans la gestion des risques
4. La mise en œuvre au sein de l'entreprise d'une politique de sécurité
5. Des règles pratiques de mise en œuvre de la sécurité: pour le télétravail, clean desk policy etc.

5.3. Charte de bonne conduite

Contenu

Contenu:

6. L'importance du facteur humain (sécurité liés au ressources humaines)
7. L'importance d'une gestion précise des actifs (classification/usage des données et support)
8. Les règles mis en œuvre pour les accès (physique et logique à l'information)
9. L'usage de moyens de chiffrement
10. Règles spécifiques d'utilisation des moyens informatiques (PC, mobile, tablette, réseaux, etc.)
11. Gestion des fournisseurs
12. Gestion des incidents de la continuité…
13. Les mesures de gestion de la conformité : surveillance des systèmes, sanctions, etc.

5.3. Charte de bonne conduite

Organisation pratique de l'atelier

Que faire avant l'atelier « charte de bonne conduite »

- Adapter ou rédiger pour votre entreprise la charte en prenant appui sur le modèle
- Noter l'ensemble des questions qui se poseraient et nous les transmettre (RGPD@itrust.lu)

Que ferons-nous pendant l'atelier « charte de bonne conduite »

- Nous traiterons l'ensemble des questions reçues pour vous aider à finaliser vos chartes en
  - replaçant la question dans le cadre de la réglementation
  - en proposant une ou plusieurs solutions
- Nous vous proposerons de vous guider dans l'encodage individuel de vos chartes (accompagnement au cas par cas) durant l'atelier
- Nous répondrons aux questions supplémentaires ou initierons des réflexions en fonctions des exemples

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

5.4. Consentement

5.4. Consentement

Organisation pratique de l'atelier

Préparation

- Identifier les traitements qui sont fondés (ou qui devraient être fondés) sur le consentement
- Vérifier que ce consentement a été donné par la personne et qu'il est inclus dans le domaine d'application de la notice et sinon l'inclure.
- Préparer la modalité de recueillement et d'annulation du consentement (y compris en termes d'information sous forme de mail, de note sur site web ou sur les contrats de service, etc.)
- Noter l'ensemble des questions qui se poseraient et nous les transmettre (RGPD@itrust.lu)

Contenu

Nous vous proposerons en complément de la formation initiale des exemples (corrects ou non) de consentement et de gestion du consentement afin d'approfondir par des exemples la formation

- Nous traiterons l'ensemble des questions reçues pour vous améliorer soit la formulation soit les moyens de gestion du consentement.
- Nous répondrons aux questions supplémentaires ou initierons des réflexions en fonctions des exemples

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Améliorer sa conformité : ateliers supplémentaires

Autres ateliers

Fondement dans le réglement

En plus des ateliers déjà programmer (et en fonction de vos besoins, de votre intérêt **et des inscriptions**), la FdA en partenariat avec itrust consulting, pourra organiser 4 autres ateliers:

- **Gestion et notification des violations de sécurité:** mettre en œuvre les obligations suivantes

Art 33-1: En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.
Art 33-2: Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

- **Gestion des sous-traitants et clauses contractuelles:** mettre en œuvre les obligations suivantes

Art 28-1: Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée.
Art 28-2: Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

- **Classification des données et procédures afférentes:** car protéger les données à caractère personnel, c'est avant tout savoir identifier et gérer ces données
- **Gestion documentaire:** Le RGPD induit la mise en œuvre de documents qu'il faut savoir gérer : mise à jour, distribution, etc.

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Question?

Si vous voulez nous contacter:
Carlo Harpes : harpes@itrust.lu
Matthieu Aubigny: aubigny@itrust.lu

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Merci de votre attention

Si vous voulez nous contacter:
Carlo Harpes : harpes@itrust.lu
Matthieu Aubigny: aubigny@itrust.lu