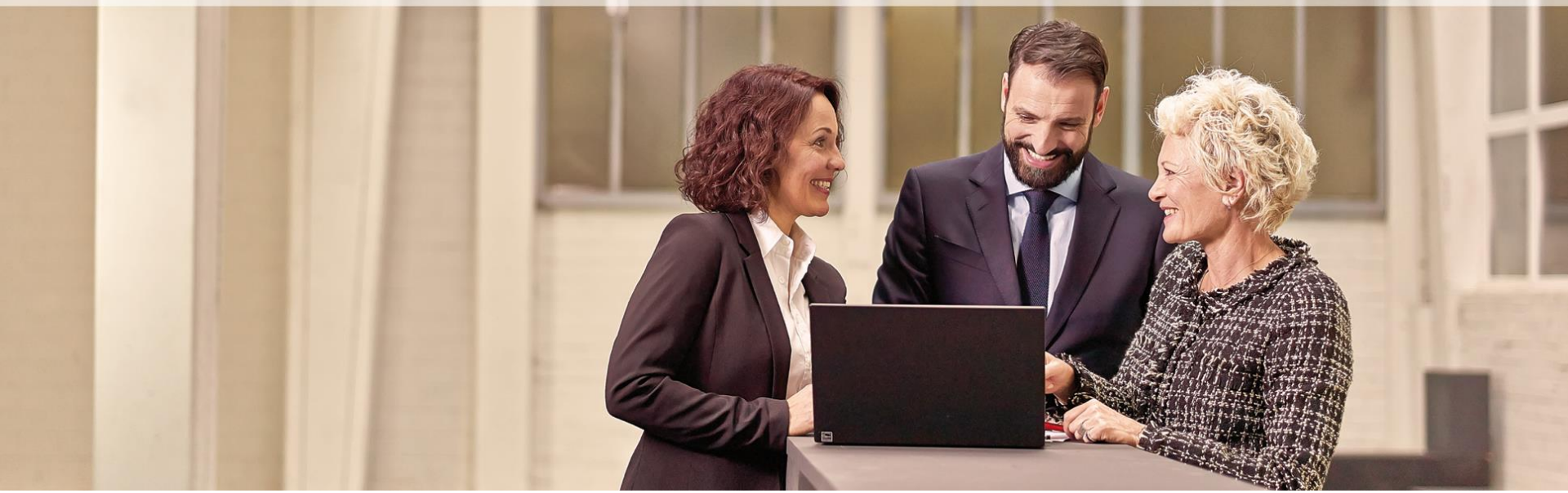
Nouveau règlement général sur la protection des données de l'Union européenne et révision de la loi fédérale sur la protection des données : enjeux et répercussions pour les entreprises basées en Suisse



CONFERENCE

Nicolas Duc
Alessandro Oberti

Genève, le 27 avril 2018

Audit | Fiduciaire | Fiscalité | Conseil

BDO

LES GRANDS PRINCIPES DE LA PROTECTION DES DONNÉES

Nicolas Duc
Membre de la Direction Régionale Suisse Romande
Partner, Responsable ligne de produits Fiscalité et Droit
BDO Suisse romande

COMMUNICATION CLIENTS

Vous avez sans doute reçu récemment des mails émanant de vos fournisseurs informatiques tels que  ou 

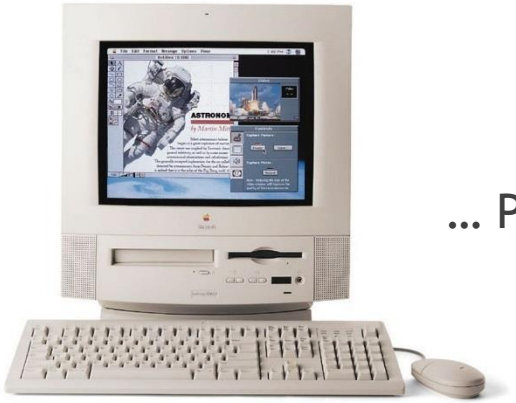
vous invitant à consulter leurs conditions d'utilisation et visant à vous rassurer quant à l'utilisation de vos données personnelles.

DIRECTIVE 95/46/CE (24.10.1995)

La Directive 95/46/CE a été édictée en 1995

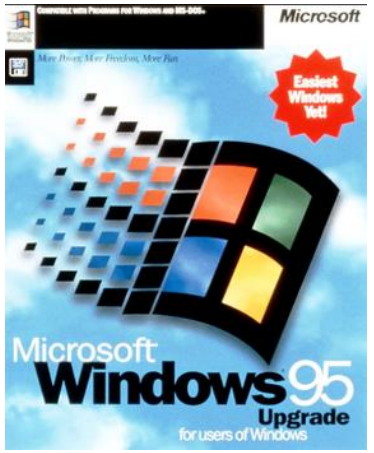
La même année…

… Siemens S3 avec SMS …



… Processeur de 66MHz et 80 MB de capacité du disque dur…

… Windows 95 …



DVD TM

CLARIFICATION

Acronymes utilisés

RÈGLEMENTS **RGPD**

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril 2016

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(Gesetzgebungsakte)

REGOLAMENTI **RGPD**

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

VERORDNUNGEN **DSGVO**

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

REGULATIONS **GDPR**

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

ÉVOLUTION LÉGISLATIVE

UNION EUROPÉENNE

- Directive (UE) 2016/680 adoptée le 27 avril 2016
- Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données à caractère personnel
- Projet de convention STE 108 du Conseil de l'Europe
- Délai transitoire de 2 ans et entrée en vigueur le **25 mai 2018**
- La directive UE 2016/680 est «self executing» => pas besoin de la mettre en œuvre au niveau du droit national

SUISSE

- Décembre 2016 : avant-projet de révision en consultation
- 15 septembre 2017 : message du Conseil fédéral pour une révision totale de la LPD et modification d'autres lois fédérales
- Trois objectifs :
  - Renforcer les dispositions légales de protection des données pour faire face au développement fulgurant des nouvelles technologies
  - Tenir compte des réformes de l'UE et du Conseil de l'Europe
  - Maintien de la compétitivité de la Suisse

ENJEUX POLITIQUES EN SUISSE

Loi sur la protection des données. Révision totale et modification d'autres lois fédérales (17.059)

- Le Conseil fédéral a transmis au Parlement le 15.09.2017 un message visant à réviser totalement la LPD.
- La Commission des institutions politiques du Conseil national (CIP-N) a adopté le 12.01.2018 une motion d'ordre demandant la scission du projet, afin d'examiner tout d'abord la mise en œuvre du droit européen qui, en vertu des Accords de Schengen, doit avoir lieu dans un délai donné. La CIP-N pourra ensuite s'atteler à l'examen de la révision totale de la LPD sans être contrainte par le temps.
- La CIP-N a décidé le 13.04.2018 de réviser en deux étapes le droit de la protection des données et a séparé le projet en deux parties. Dans un premier temps, elle a adapté la législation suisse aux exigences du droit européen. Elle souhaite désormais s'atteler immédiatement à la deuxième étape de la révision, qui prévoit la révision totale de la LPD et s'applique à tout traitement de données par des personnes privées ou par des organes fédéraux. Elle a prévu d'organiser des auditions supplémentaires sur le sujet à l'une de ses prochaines séances.
- Le Conseil national examinera les adaptations de la législation effectuée sur la base de la Directive européenne à la session d'été et décidera parallèlement s'il approuve la scission du projet de révision du droit de la protection des données.

QUELQUES DEFINITIONS ET PRINCIPES DE BASE

- **Données personnelles (art. 4 lit. a P-LPD)**
  - Personnes physiques uniquement
  - Numéro identification, données de localisation, identité physique, génétique, économique, culturelle, sociale
  - Ex: n° AVS, n° tél, adresse, état civil
  - Exception: données anonymisées
- **Données personnelles sensibles (art. 4 lit. c P-LPD)**
  - Données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales; données sur la santé, la sphère intime, l'origine raciale ou ethnique; données génétiques et biométriques (identifiant une personne physique de façon unique); données sur des poursuites, sanctions pénales et administratives; données sur des mesures d'aide sociale

QUELQUES DEFINITIONS ET PRINCIPES DE BASE

- **Activité de traitement (art. 4 lit. d P-LPD)**
  - Toute opération relative à des données personnelles: collecte, enregistrement, conservation, utilisation, modification, communication, archivage, effacement, destruction
- **Profilage (art. 4 lit. f P-LPD)**
  - Evaluation automatisée à des fins d'analyse de la situation économique, du comportement, des préférences, de la localisation, etc.

QUELQUES DEFINITIONS ET PRINCIPES DE BASE

- **Exceptions à l'application de la loi (art. 2 P-LPD)**
  - Traitement de données personnelles par une personne physique pour un usage exclusivement privé (art. 2 al. 2 lit. a P-LPD)
  - Procédures (art. 2 al. 3 P-LPD)
  - Registres publics (art. 2 al. 4 P-LPD)
- **Conseiller à la protection des données personnelles (art. 9 P-LPD)**
  («Data Protection Officer» - délégué à la protection des données (RGPD)
  - «Gardien du temple»
  - RGPD: obligation; P-LPD: pas d'obligation pour les entreprises

QUELQUES DEFINITIONS ET PRINCIPES DE BASE

- **Protection des données dès la conception («privacy by design»; art. 6 al. 1 P-LPD)**
  - Intégrer exigences LPD dès l'origine
  - Dans le système IT (ex: outil KYC, etc.)
- **Protection des données par défaut («privacy by default»; art. 6 al. 3 P-LPD)**
  - Préréglages: traitement limité au minimum requis par la finalité poursuivie
- **Registre des activités de traitement (art. 11 P-LPD)**
  - Exception pour les entreprises qui ont moins de 50 collaborateurs
- **Analyse d'impact (art. 20 P-LPD)**
  - Principe: obligatoire pour tout traitement
  - Exception: LBA, lutte contre le terrorisme

QUELQUES DEFINITIONS ET PRINCIPES DE BASE

- **Principe de base (art. 5 P-LPD)**
  - Licéité
  - Proportionnalité : que le strict minimum
  - Finalité : quel but? KYC, LBA, gestion portefeuille
  - Conservation: durée et support
  - Exactitude: mise à jour
  - Consentement (exprès en cas de données sensibles ou de profilage)
- **Exceptions au devoir d'informer et restrictions (art. 18 P-LPD)**
  - Personne déjà informée (ex: CGV)
  - Base légale: LBA, CDB 16, LCC
  - Obligation de garder le secret

QUELQUES DEFINITIONS ET PRINCIPES DE BASE

- **Motifs justificatifs en cas d'atteinte d'illicite (art. 27 P-LPD)**
  - Contrat, concurrence
  - Solvabilité (cas Moneyhouse)
    - OK si 4 conditions sont remplies:
      - Pas de données sensibles, ni profilage
      - Communication limitée
      - Max 5 ans
      - Personne majeure

AU NIVEAU EUROPÉEN

- **Contraignant pour toute l'UE**
  La directive est directement applicable à tous les Etats-membres ; les Etats sont libres de prévoir des règles plus strictes

- **Amendes plus sévères**
  jusqu'à 4% du chiffre d'affaires annuel de tout le groupe !

- **Devoir d'annonce en cas de violation**
  «Incident Reporting» dans les 72 heures

- **Exemption formelle mais non effective pour les PME**

QUID EN SUISSE ?

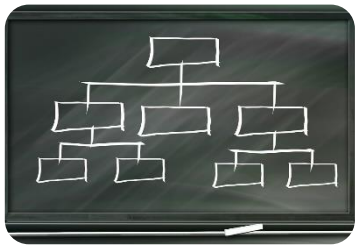
- **Devoir de documentation**
  En particulier pour **l'analyse d'impact**
- Favoriser **l'autoréglementation**
- **Devoir d'annonce en cas de violation («dans les meilleurs délais»)**
- **Renforcement des sanctions pénales (amendes jusqu'à KCHF 250)**
- Suppression de la protection des données des personnes morales

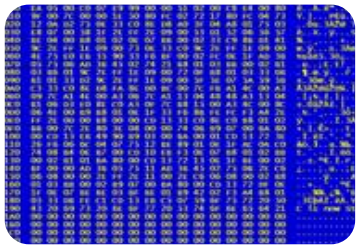
INVENTAIRE ET CLASSIFICATION DES DONNEES

Alessandro Oberti
Senior Manager
Auditeur IT et Business Process Analyst
BDO Suisse romande

RÉFÉRENTIEL

Interconnexion entre les domaines juridique, organisationnel et informatique





Licéité Bona Fides Proportionnalité Finalité Reconnaissabilité Exactitude	Mesures d'organisation adéquates	Sécurité du système d'information Mesures techniques adéquates

Collecte	Communication	Exploitation	Modification	Conservation Archivage	Destruction

FIL ROUGE

- Inventaire des données
- Analyse d'impact sur les données
- Mise à jour des règles internes
- Définition des propriétaires des données (data owner) et responsables de traitement, contrôles à effectuer, gestion des incidents, mesures de correction
- Mise à jour des contrats

APPROCHE : INVENTAIRE DES DONNÉES

Papier et/ou électronique

1. Quelles sont les données utilisées ?

2. Par qui et comment le sont-elles ?

3. Quels sont les supports utilisés ?

4. Quels sont les contrôles sur ces données ?

APPROCHE : INVENTAIRE DES DONNÉES

Papier et/ou électronique

Données «classiques» :

- Données des employés
- Données des clients
- Données de prospects
- Données utilisées par le marketing
- Données de partenaires

Exemples de types de données :

- Vidéo-surveillance
- Biométriques (contrôle d'accès)
- Cookies (sites internet)
- Enregistrements téléphoniques

APPROCHE : CLASSIFICATION DES DONNÉES

Papier et/ou électroniques

1. Quelles sont les données soumises à protection ?
   - ⇒ législation spécifique
   - ⇒ RGPD/LPD
2. Comment effectuer le traitement des données (selon quels principes ?)
   - ⇒ Licéité, Bona Fides, Proportionnalité, Finalité, Reconnaissabilité, Exactitude
3. Classification des données
4. Quid de transfert de données au sein d'un groupe ?
   - ⇒ BCR (Binding Corporate Rules)
5. Bonnes pratiques

APPROCHE : INVENTAIRE DES DONNÉES

Papier et/ou électroniques

Les entreprises helvétiques devront respecter le RGPD si elles traitent les données personnelles d'individus situés sur le territoire de l'UE et si les activités de traitement sont liées, alternativement:

1. A une offre de biens ou de services à ces individus (avec un paiement ou non à la clé).
2. Au suivi du comportement de ces individus: concernant des comportements qui ont lieu dans les pays membres de l'UE (art. 3 al. 2 let a et b RGPD).

Pour déterminer si les activités d'une entreprise sise en dehors de l'UE tombent dans le champ d'application du RGDP, les conseillers juridiques doivent analyser si **l'intention** de vendre des biens ou services dans l'UE est manifeste. Divers indices peuvent ainsi être étudiés (par exemple: la mention sur le site internet de clients situés dans les pays membres ou d'une monnaie courante dans l'UE). Dans le cas de l'art. 3 al. 2 let. b RGPD, ces experts peuvent analyser s'il existe **une volonté** claire de suivre le comportement d'individus dans l'espace européen (par exemple, en observant l'utilisation de techniques de profilage ou de Google analytics).

https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/gestion-pme/e-commerce/reglementation-ue-pour-la-protection-des-donnees.html

APPROCHE : INVENTAIRE DES DONNÉES

Papier et/ou électroniques

- Données des employées (CH + frontaliers €)
  => non soumis (considérant 23+24) + art 3 RGPD (extraterritorialité)
- Données des clients (CH, résidents au sein de l'€)
  => soumis si personnes physiques + profilage
- Données de prospects (CH, résidents au sein de l'€)
  => soumis si personnes physiques + profilage
- Données utilisées par le marketing (interne/externe)
  => soumis si personnes physiques + profilage
- Vidéo-surveillance
  => soumis
- Biométriques (contrôle d'accès)
  => soumis
- Par qui ? Comment ?
  Pour combien de temps ?

BCR (BINDING CORPORATE RULES)

Définissent la politique d'une entreprise en matière de transfert de données personnelles.

Permettent d'offrir une protection adéquate aux données transférées

Art. 47 let. a

… ces règles soient juridiquement contraignantes, et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés ; …

CODE DE CONDUITE

ANALYSE D'IMPACT

PIA : cette analyse doit permettre de répondre à ces questions :

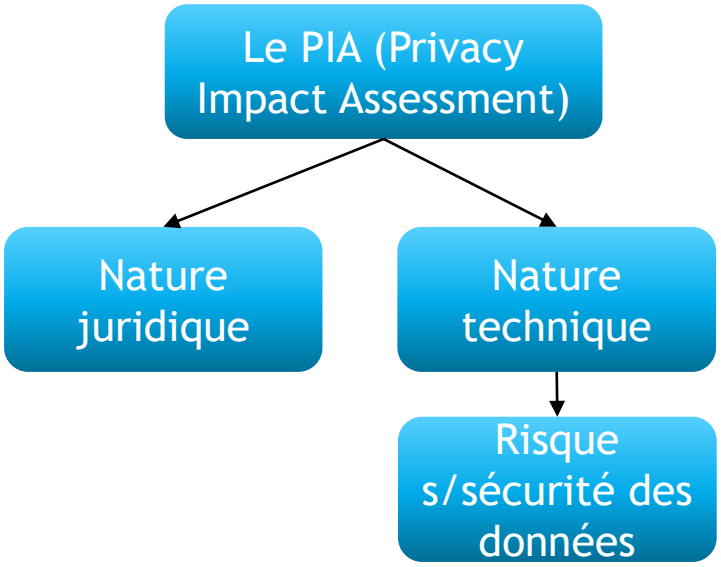
- Quels sont les éléments à protéger ?
  - Quid de chiffrer les données, pseudonymisation, limiter les données…?
- Quels sont les impacts potentiels ?
  - Soustraction d'information, modification des données…
- Quelles sont les sources de risques ?
  - Gestion des accès et des ressources, tests de vulnérabilités, pen test…
- Quels sont les supports utilisés ?
  - Disque dur, papier, infrastructure du SI…

ANALYSE D'IMPACT

Privacy Impact Assessment

Art. 35

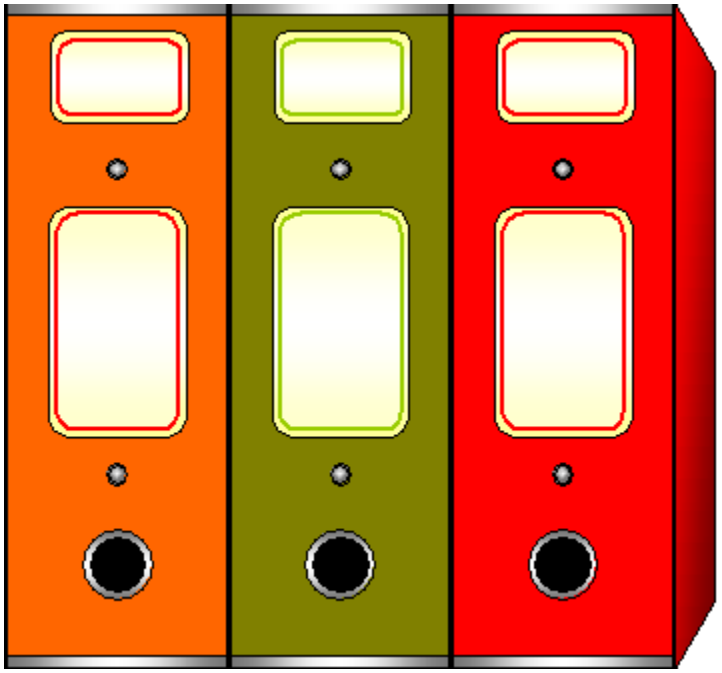
Le PIA doit obligatoirement être mené quand le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.



REGISTRES

3 REGISTRES DOIVENT ÊTRE DEFINIS:

- Un registre de traitement
- Un registre pour les corrections (mises à jour des données)
- Un registre faisant état des notifications (data breach)



REGISTRE DE TRAITEMENT

tableau qui récapitule les informations à faire figurer pour chaque traitement.

	Information à faire figurer	Responsable de traitement	Sous-traitant
Qui ?	Nom et coordonnées du responsable de traitement et de son représentant le cas échéant (et DPO le cas échéant)	☑	☑
	Nom et coordonnées du sous-traitant		☑
Pourquoi ?	Finalités du traitement	☑	
	Catégories de traitement		☑
Quoi ?	Personnes concernées et catégories de données concernées	☑	
Où ?	Destinataires	☑	
	Transfert vers un pays tiers ou organisation internationale	☑	☑
Jusqu'à quand ?	Délais de conservation et d'effacement des données	☑	
Comment	Description de mesures de sécurité techniques et organisationnelles	☑	☑

Source: MARCEAU Avocats, Paris

REGISTRE DE TRAITEMENT

Exemple proposé par la CPVP (Belgique)

1	**Registre des activités de traitement**					
2	**Responsable du traitement :**					
12	**Délégué à la protection des données :**					
18						
19	**processus opérationnel/traitement**	**description fonctionnelle du traiten**	**données utilisées et personnes conc**	**sous-traitant**	**échange de données**	**technologie**
20	identification du processus opérationnel *nom, propriétaire du processus* *(dans la colonne ci-dessous, on reprend le nom du traitement en fonction de la lisibilité de la version électronique du registre)*	identification et information au sujet du traitement *numéro , , description fonctionnelle, , finalité, fondement du traitement, type de traitement et description fonctionnelle*	détails sur les données traitées et sur les personnes concernées dont les données sont traitées *catégorie fonctionnelle, catégorie sensible de traitement de données, catégorie de personne concernée, niveau de classification, délai de conservation, source authentique*	identification du sous-traitant (externe à l'organisation) impliqué dans le traitement *nom, n° du contrat de traitement de données*	informations au sujet d'un éventuel échange de données avec des tierces parties. catégorie(s) de données, *catégorie(s) de destinataires, pays tiers/organisation internationale, documents garanties appropriées*	description de la technologie, des applications et du logiciel employés pour le traitement.

	A
5	**Liste indicative de types de finalités**
83	**Fondement du traitement**
91	**Liste indicative des catégories de données fonctionnelles**
196	**type de traitement**
206	**catégorie de données RGPD**
223	**liste indicative de catégorie(s) de destinataires**
236	**nature de la transmission vers un pays tiers/une organisation internationale**
243	

Colonne dans le canevas	Rubrique dans la déclaration
traitement	1. dénomination du traitement
finalité du traitement	2. finalité ou ensemble de finalités liées pour lesquelles des données sont traitées
fondement du traitement	4. base(s) légale(s) ou réglementaire(s)
catégorie de données fonctionnelle	3. catégories de données qui sont traitées
catégorie de personnes concernées	information non reprise dans les déclarations
délai de conservation	10. délai de conservation prévu
catégorie de données	5. Catégories de destinataires et catégories de données qui peuvent être fournies
Catégorie(s) de destinataires	5. Catégories de destinataires et catégories de données qui peuvent être fournies
pays tiers/organisation internationale	12. données envoyées à l'étranger
documents garanties appropriées	6. quelles mesures sont prises pour sécuriser la communication de données à des tiers ? (attention, uniquement s'il est question de la situation de l'article 49.2 du RGPD)
description des mesures de sécurité	11. description générale des mesures de sécurité 6. quelles mesures sont prises pour sécuriser la communication de données à des tiers ? (si transfert de données)
information des personnes concernées	7. comment les personnes concernées sont-elles informées de l'enregistrement de leurs données ?
procédure d'exercice des droits	9. Mesures spécifiques pour l'exercice des droits

CPVP
Commission de la protection de la vie privée

BDO

REGISTRE DE TRAITEMENT

Exemple proposé par la CNIL (France)

Identification du traitement				Acteurs	Finalité du traitement	Transferts hors UE ?	Données sensibles ?
Nom / sigle	N° / REF	Date de création	Dernière mise à jour	Responsable du traitement	Finalité principale	Oui /non	Oui/non

CNIL.

Numéro d'identification national unique (NIR pour la France)	

Catégories de personnes concernées	Description
Catégorie de personnes 1	
Catégorie de personnes 2	

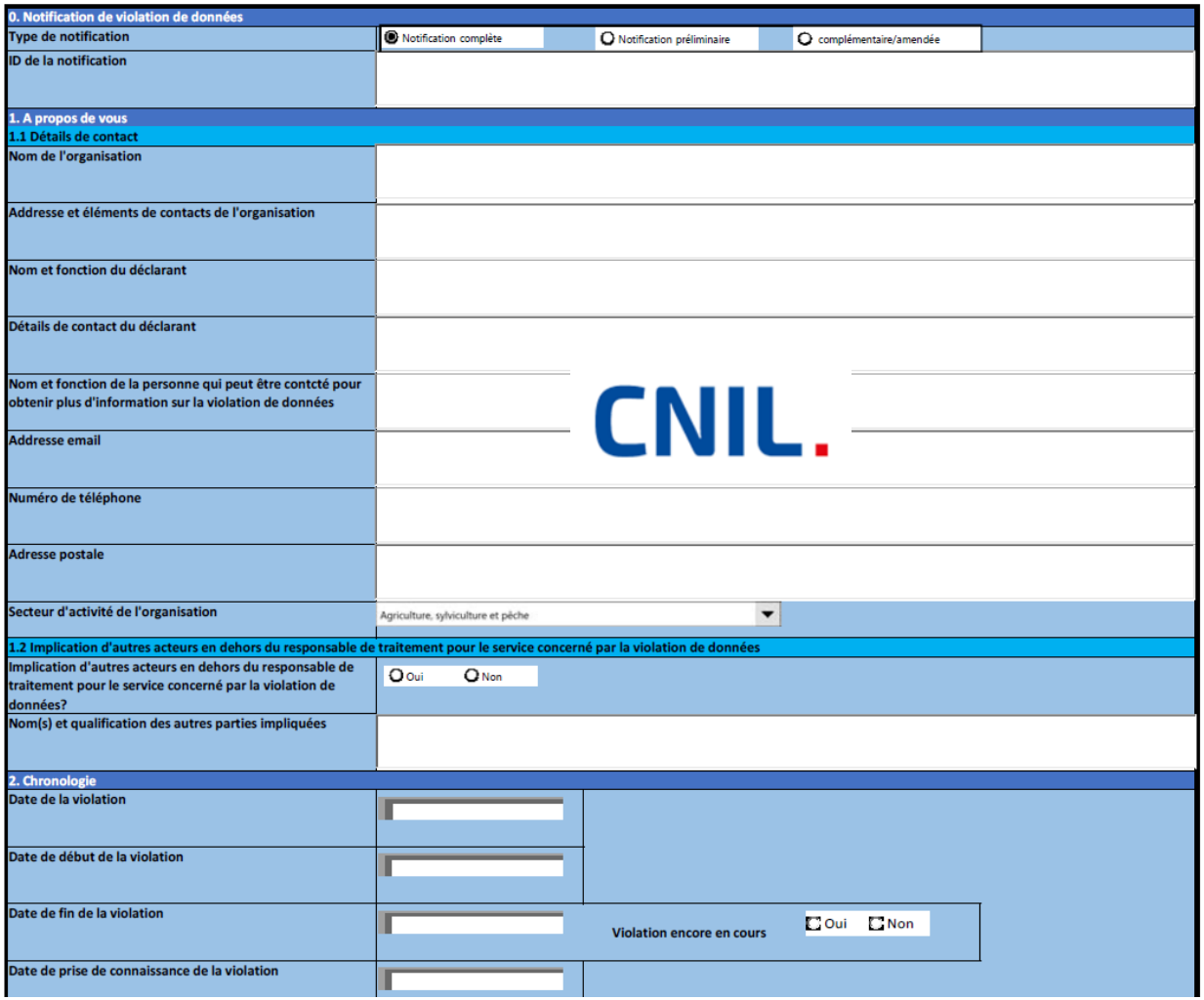
Destinataires	Description	Type de destinataire
Destinataire 1		
Destinataire 2		
Destinataire 3		
Destinataire 4		

Tranferts hors UE	Destinataire	Pays	Type de Garanties	Lien vers le doc
Organisme destinataire 1				
Organisme destinataire 2				
Organisme destinataire 3				
Organisme destinataire 4				

rôles	Délai d'effacement		CCT		Pays			Personnes concernées par les traitements			Service interne qui traite les données					
Responsable de traitement			BCR		France	UE		Clients			Sous-traitants					
Représentant du responsable de traitement			Pays adéquat		Autriche	UE		Administrés			Destinataires dans des pays tiers ou organisations internationales					
											Partenaires institutionnels ou commerciaux					
Co-responsable de traitement			Privacy shield		Belgique	UE		Salariés			Autre (Préciser)					
Représentant du co-responsable de traitement			Code de conduite		Bulgarie	UE		Candidats								
Délégué à la protection des données			Certification		Chypre	UE										
Sous-traitant			Dérogations (art 49)		Croatie	UE										
					Danemark	UE										
					Espagne	UE										
					Estonie	UE										

BDO

REGISTRE DE NOTIFICATION

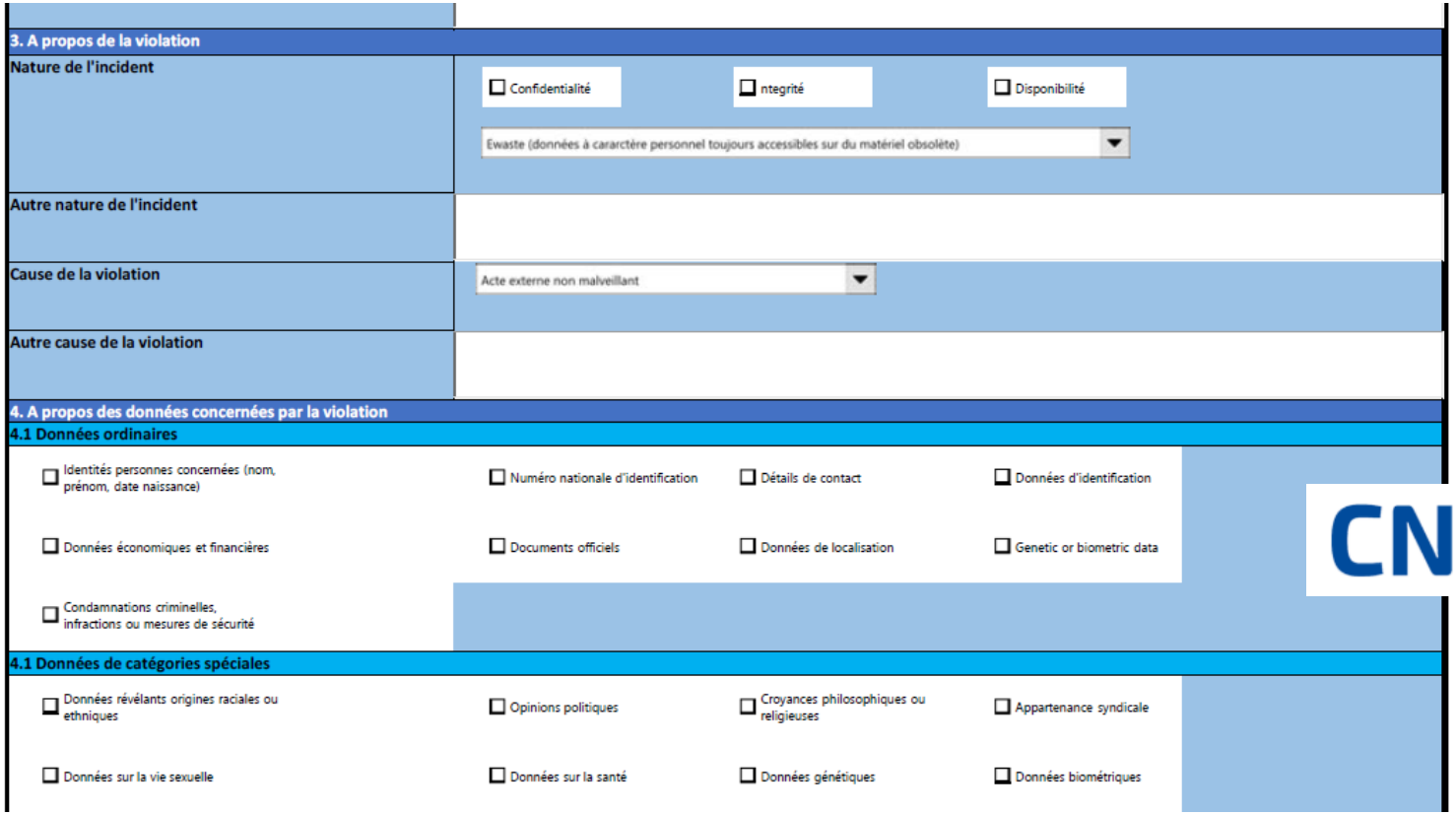


0. Notification de violation de données	
Type de notification	◉ Notification complète ○ Notification préliminaire ○ complémentaire/amendée
ID de la notification	
1. A propos de vous	
1.1 Détails de contact	
Nom de l'organisation	
Addresse et éléments de contacts de l'organisation	
Nom et fonction du déclarant	
Détails de contact du déclarant	
Nom et fonction de la personne qui peut être contcté pour obtenir plus d'information sur la violation de données	
Addresse email	
Numéro de téléphone	
Adresse postale	
Secteur d'activité de l'organisation	Agriculture, sylviculture et pêche
1.2 Implication d'autres acteurs en dehors du responsable de traitement pour le service concerné par la violation de données	
Implication d'autres acteurs en dehors du responsable de traitement pour le service concerné par la violation de données?	○ Oui ○ Non
Nom(s) et qualification des autres parties impliquées	
2. Chronologie	
Date de la violation	
Date de début de la violation	
Date de fin de la violation	Violation encore en cours ☐ Oui ☐ Non
Date de prise de connaissance de la violation	

CNIL.

BDO

REGISTRE DE NOTIFICATION



3. A propos de la violation	
Nature de l'incident	☐ Confidentialité ☐ ntegrité ☐ Disponibilité Ewaste (données à cararctére personnel toujours accessibles sur du matériel obsolète)
Autre nature de l'incident	
Cause de la violation	Acte externe non malveillant
Autre cause de la violation	

4. A propos des données concernées par la violation			
4.1 Données ordinaires			
☐ Identités personnes concernées (nom, prénom, date naissance)	☐ Numéro nationale d'identification	☐ Détails de contact	☐ Données d'identification
☐ Données économiques et financières	☐ Documents officiels	☐ Données de localisation	☐ Genetic or biometric data
☐ Condamnations criminelles, infractions ou mesures de sécurité			
4.1 Données de catégories spéciales			
☐ Données révélants origines raciales ou ethniques	☐ Opinions politiques	☐ Croyances philosophiques ou religieuses	☐ Appartenance syndicale
☐ Données sur la vie sexuelle	☐ Données sur la santé	☐ Données génétiques	☐ Données biométriques

CNIL.

BDO

DIRECTIVES INTERNES, RÈGLES ET CONTRÔLES

Assurer un degré de conformité adéquat quant aux règles internes

- Règles de gestion des accès aux données
- Surveillances sur les processus internes définis (contrôles internes et monitoring)
- Gestion des incidents, reporting interne et communication aux instances concernées + clients
- Formaliser les processus internes
- Garantir un suivi de la technologie (sécurité du système d'information)
- Garantir un processus de rectification et de destruction (droit à l'oubli)

SITE INTERNET

LES OBLIGATIONS LÉGALES EN MATIÈRE DE COOKIES

Avant de déposer ou lire un cookie, les éditeurs de sites ou d'applications doivent :

- informer les internautes de la finalité des cookies obtenir leur consentement
- fournir aux internautes un moyen de les refuser.
- La durée de validité de ce consentement est de 13 mois maximum.
- L'obligation de recueil du consentement s'impose aux responsables de sites, aux éditeurs d'applications mobiles, aux régies publicitaires, aux réseaux sociaux, aux éditeurs de solutions de mesure d'audience qui ont l'entière responsabilité de se mettre en accord avec la loi.
- Certains cookies sont cependant dispensés du recueil de ce consentement. (Il s'agit des cookies et des traceurs strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur.

SITE INTERNET

Gestion des cookies par le tag management.

L'avantage est de centraliser les consentements des visiteurs de votre site internet.

```
<head>
<script type="text/javascript" src="/tarteaucitron/tarteaucitron.js"></script>
<script type="text/javascript">
 tarteaucitron.init({
"hashtag": "#tarteaucitron", /* Ouverture automatique du panel avec le hashtag */
"highPrivacy": false, /* mettre à true désactive le consentement implicite */
"orientation": "top", /* le bandeau doit être en haut (top) ou en bas (bottom) ? */
"adblocker": false, /* Afficher un message si un adblocker est détecté */
"showAlertSmall": true, /* afficher le petit bandeau en bas à droite ? */
"cookieslist": true, /* Afficher la liste des cookies installés ? */
"removeCredit": false /* supprimer le lien vers la source ? */ }) ;
</script>
</head>
```

Site de Google: script pour éviter de tracer la publicité
https://support.google.com/dfp_premium/answer/3202794?hl=fr

Exemples de solutions commerciales :

- Audito
- BayCloud,
- FiftyFive,
- Evidon,
- Havas (Central Tag),
- TagCommander,
- TarteAuCitron,
- TRUSTe

Et une solution open source :

- tarteaucitron.js

SITE INTERNET

Consentement

Article 4 n°11 du RGPD : « (…) « 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 ; (…) »

Les nouvelles conditions d'utilisation sont formelles : "Pour utiliser WhatsApp, vous devez avoir au moins 16 ans." Jusqu'à présent réservée aux personnes de plus de 13 ans, l'application de messagerie relève l'âge minimum d'utilisation en Europe (24 avril 2018).

Article 8 du RGPD :

« 1. (…) le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.

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. (…) »

BONNES PRATIQUES

Identifier les données soumises à protection et les référencer selon un label permettant de les reconnaître. Il sera différent de la classification interne de degré de confidentialité

ByOD : Bring your Own Device

=> Faire signer un consentement pour le respect des règles et mesures internes (contrôles possibles)

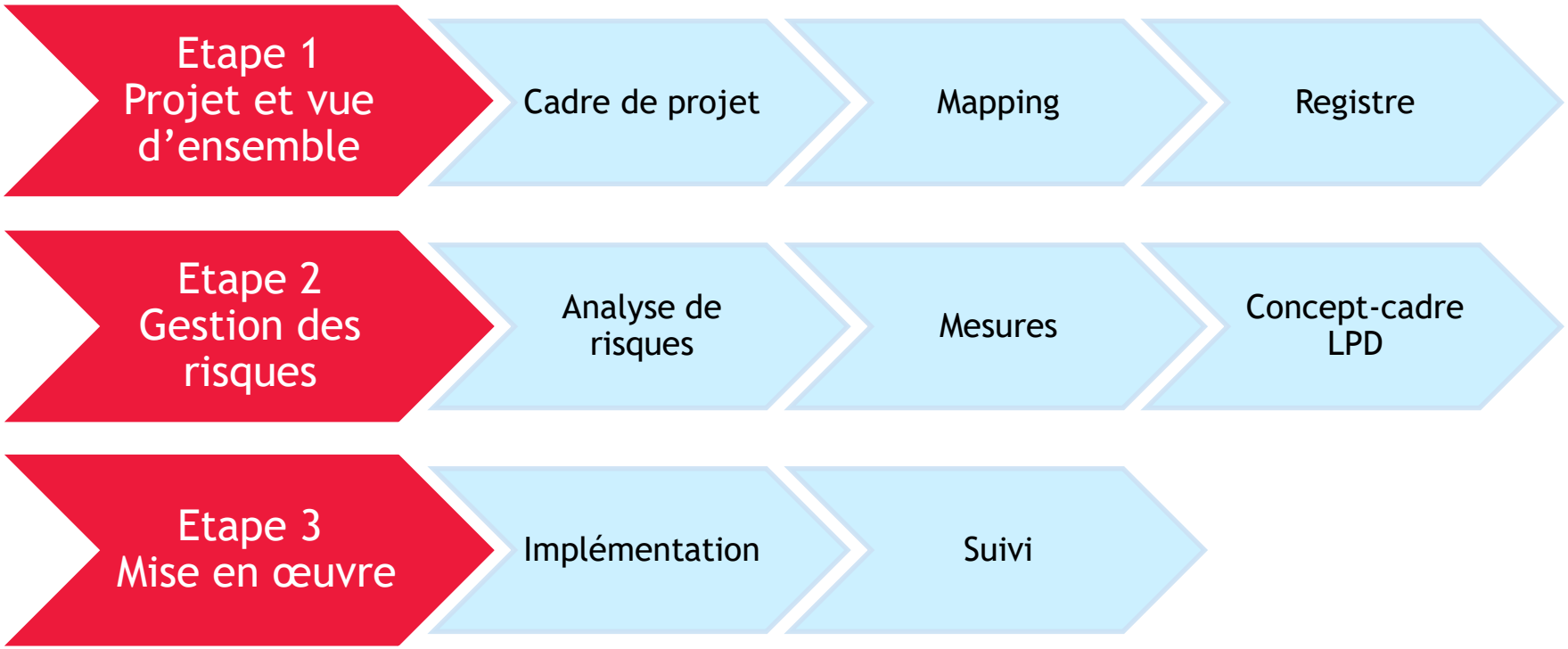
RGPD/LPD	Classification Interne
Téléphone	CID
E-mail	Interne
#Passeport	Confidentielle
Biométrique	Secrète

BONNES PRATIQUES

- Limiter les bases de données soumises à protection et centraliser les accès
- N'autoriser que l'utilisation du système d'information à titre professionnel
- Limiter les supports de données
- Limiter les applications et interfaces qui ne permettent pas de garantir un degré de traçabilité adéquat (accès)
- Vérifier le respect des règles internes
- Garantir un degré de surveillance adéquat par rapport aux types de données récoltées et conservées (monitoring)
- Emettre un «tag» identifiant la durée de vie de la donnée à conserver

PROTECTION DES DONNÉES ET RGPD

Approche proposée par BDO



EN RÉSUMÉ

Nos propositions de solutions

	1. CADRE PROJET, REGISTRE, MAPPING	2. GESTION DES RISQUES	3. IMPLEMENTATION ET SUIVI
Objectifs	▶ Projet structuré et documenté ▶ Vue d'ensemble ▶ Transfert de know-how aux responsables de domaines d'activités ▶ Production d'un Registre de traitement (exigence légale)	▶ Analyse de risque structurée et documentée (exigence légale) ▶ Définition des mesures techniques et organisationnelles ▶ Concept cadre de protection des données documenté de manière claire et synthétique	▶ Implémentation du concept cadre mesures techniques et organisationnelles ▶ Approfondissement de l'analyse des processus particulièrement sensibles ▶ Coordination avec l'implémentation d'autres projets
Prestations BDO	▶ Support à la gestion de projet ▶ Workshop avec les responsables d'unités organisationnelles • Introduction à la protection des données • Explications et support pour l'établissement du registre ▶ Mapping des principaux systèmes de données de la Banque	▶ Workshop/support des responsables concernant l'établissement du niveau de risque des processus ▶ Coordination avec les exigences réglementaires du domaine bancaire et financier ▶ Proposition de mesures techniques et organisationnelles	▶ Expertise Regulatory & Compliance pour la coordination, l'identification de synergies et de conflits éventuels ▶ Revue des processus d'externalisation ou de transferts de données à l'étranger et des garanties contractuelles (outsourcing) ▶ Expertise Juridique et Technique/IT pour l'implémentation des mesures
Tools	▶ Formations RGPD/LPD ▶ Modèle de registre ▶ Instructions pour le registre et support	▶ Modèle pour l'analyse de risque ▶ Liste des mesures organisationnelles et techniques possibles ▶ Concept-cadre	▶ Liste des principales exigences réglementaires à coordonner ▶ Mise à disposition de modèles en matière d'outsourcing

RECOMMANDATIONS

https://www.cnil.fr

QUESTIONS – RÉPONSES

MERCI POUR VOTRE ATTENTION

NICOLAS DUC
Dr. en droit,
Partner, Responsable ligne de produits Fiscalité et Droit
BDO Suisse romande

Direct: +41 21 310 23 84
E-Mail: nicolas.duc@bdo.ch

ALESSANDRO OBERTI
Senior Manager, Auditeur
Responsable IT & Business Analyste
BDO Suisse romande

Direct: +41 22 322 24 95
E-Mail: alessandro.oberti@bdo.ch