EU GDPR Roadmap Belgium

POINT D'ACTION 1 : examen et adaptation de la réglementation en général

CONTEXTE ET OBJECTIFS

- rendre la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et toute autre réglementation pertinente conforme au Règlement européen (GDPR) et à la Directive 216/80 (impact à vérifier par les services d'inspection sociale)
- si nécessaire, rédaction de nouvelles dispositions qui prévoient des exceptions supplémentaires pour le secteur public

ACTIONS ET TIMING

Actions **Rouge: il est crucial d'un point de vue stratégique de réaliser l'action dans les délais**	**Ligne du temps**	**R**esponsible **C**onsulted **S**upportive **I**nformed
○ là où nécessaire, adaptation de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Règlement a un effet direct) - la suppression de la déclaration - la notification des incidents de sécurité - la compétence de contrôle et de sanction - l'obligation de documentation de l'inventaire et de l'analyse d'impact relative à la protection des données - les dispositions en matière de consultation, de concertation et de collaboration avec l'autorité de contrôle - le mécanisme du code de bonne conduite et de la certification éventuelle - le statut du coordinateur responsable pour la protection des données à caractère personnel (DPO) (maintien du cumul actuel avec le conseiller en sécurité) - analyse et, le cas échéant, rédaction d'exceptions légales supplémentaires pour le secteur public et de règles relatives à l'imposition (la non-imposition) de sanctions administratives pour le secteur public - la possibilité de prévoir des conditions supplémentaires pour le traitement de données génétiques, biométriques ou de données relatives à la santé, ...	T3 2017 (plus tôt pour ce qui concerne certains aspects?)	**R: SPF Justice** C/S : CPVP / BCSS (direction générale & section I&SD) I: IPSS
○ le redesign de la CPVP et des Comités sectoriels (voir la note du Conseil des ministres): renforcement de l'indépendance, des tâches et des missions de l'autorité de contrôle & éventuellement des compétences complémentaires par loi	T1 2018	**R: SPF Justice** C/S: CPVP / BCSS (direction générale & section I&SD) I: OISZ

POINT D'ACTION 2 : examen et adaptation de la réglementation secteur social et de la santé

CONTEXTE ET OBJECTIFS

- rendre la réglementation pertinente conforme à la GDPR;
- si nécessaire, rédaction de nouvelles dispositions qui prévoient des exceptions supplémentaires pour le secteur social et de la santé

ACTIONS ET TIMING

Actions	**Timing**	**Responsable**
○ examen conformité réglementation actuelle et exceptions; modification références légales ○ screening/inventaire des articles / de la réglementation à modifier ○ concertation au niveau interne / externe sur l'opportunité de la modification ○ rédaction adaptations terminée ○ parcourir la procédure (avis, publication)	**T4 2017** Oct 2016 Nov 2016 Juin 2017 Déc 2017	**R: IPSS & BCSS section I&SD (chacun pour sa propre réglementation)** S: BCSS/IPSS I: CPVP
○ examen de l'opportunité d'adapter l'article 23 de la GDPR: (...) limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 (...); ces exceptions légales doivent contenir des dispositions spécifiques, comme prescrit dans la GDPR ○ inventaire des exceptions possibles ○ concertation au niveau interne / externe sur l'opportunité de la modification ○ le cas échéant, rédaction d'exceptions légales supplémentaires pour le secteur social et de la santé, telles qu'en matière de - limitation du droit à la portabilité; - **notification des incidents de sécurité à l'intéressé.** ○ rédaction adaptations terminée ○ parcourir la procédure (avis, publication)	**T4 2017** Oct 2016 Nov 2016 Juin 2017 Déc 2017	**R: BCSS section I&SD** C : CPVP I: IPSS
○ adaptation de l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale et de l'arrêté royal du 20 septembre 2012 organisant la sécurité de l'information à la Plate-forme eHealth et fixant les missions et les compétences du médecin sous la surveillance et la responsabilité duquel le traitement de données à caractère personnel relatives à la santé s'effectue ○ inventaire des articles à modifier ○ concertation au niveau interne / externe sur l'opportunité de la modification ○ rédaction adaptations terminée ○ parcourir la procédure (avis, publication)	**T1 2018** Jan 2017 Fév. 2017 Sep 2017 Mars 2018	**R: BCSS section I&SD** C: CPVP I: IPSS

EU GDPR Roadmap Belgium

POINT D'ACTION 3 : étapes à suivre pour l'ensemble des institutions des secteurs social et de la santé

CONTEXTE ET OBJECTIFS

- mettre au point/préparer/adapter ensemble de mesures afin de pouvoir appliquer la nouvelle réglementation dans les délais et dans sa totalité dans l'ensemble du secteur social et du secteur de la santé;
- le responsable du traitement devra dorénavant évaluer, de manière objective, le degré de probabilité et de gravité des risques pour les droits et libertés des personnes lorsqu'il effectue un traitement; il est entièrement responsable du respect effectif des règles; il est également responsable vis-à-vis des autorités de contrôle et des personnes concernées pour ce qui concerne les mesures prises à cet égard.

ACTIONS ET TIMING

Actions	**Timing**	**Responsable**
○ **la sensibilisation des membres du staff des institutions concernées (privacy awareness)** ○ **Rôle du DPO** ▪ **Lien entre conseiller en sécurité (CISO) et privacy officer (DPO)** ○ **"EU GDPR for dummies"** ○ **Obligation de déclaration**	T1 - T4 2017	**R: BCSS (direction générale & section I&SD) & IPSS**
○ **concrétisation de la nouvelle approche basée sur le risque; détermination du niveau de risque des traitements au sein du secteur** ○ **Privacy Risk Management approche minimale**	T1 2017 Fév. 2017	**R: BCSS section sécurité** S: IPSS (concertation au sein du groupe de travail Sécurité de l'information) C : CPVP (concertation au sein du Comité européen de la protection des données)
○ **la CPVP doit établir une liste des types de traitement pour lesquels une analyse d'impact relative à la protection des données est obligatoire et peut établir une liste des types de traitement pour lesquels une analyse d'impact relative à la protection des données n'est pas obligatoire** ○ **un template et des instructions concernant l'analyse d'impact relative à la protection des données (avec respect des exceptions prévues dans la GDPR)** **accent mis sur l'obligation d'une analyse d'impact relative à la protection des données préalable pour certains types de traitements considérés comme sensibles et sur les mesures susceptibles d'être prises pour réduire ces risques; si cette analyse préalable permet de détecter des risques particuliers, le responsable du traitement devra consulter la CPVP avant d'entamer le traitement** **Avec un template et des instructions pour l'obligation de documentation**	T3 2017 T1 2018 Premier draft fin déc. 2016 Version finale fin déc. 2017	**R: CPVP** I: BCSS / IPSS **R: BCSS section sécurité** S: IPSS (concertation au sein du groupe de travail Sécurité de l'information) I: CPVP
○ **le cas échéant, actualiser/rédiger des policies concernant la collecte, la destruction, l'enregistrement et la recherche de données à caractère personnel et traitement ultérieur pour d'autres finalités (nouveau !) en conformité avec les principes de la GDPR** ○ **le cas échéant, actualiser les policies de sécurité (dont les policies relatives aux loggings, aux tests, au**	T1 2018 Premiers drafts fin déc. 2017	**R: BCSS section Sécurité & IPSS (groupe de travail Sécurité de l'information: répartition des tâches**

monitoring, au helpdesk) **quelques exemples de mesures de sécurité données par la GDPR sont la pseudonymisation, le chiffrement, des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement, des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident et une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles** ○ **actualiser les directives et les mesures de références de la CPVP**	Version finale fin avr. 2018	**sur la base des policies sur lesquelles la GDPR EU a un impact** **R: CPVP** I: BCSS
○ **une policy concernant la maîtrise, le traitement et la notification des infractions relatives aux données à caractère personnel (compte tenu des exceptions légales supplémentaires éventuelle vis-à-vis de l'intéressé; voir les points d'action 1 et 2) - à intégrer dans une approche plus large des incidents de sécurité** **En cas de violation de données à caractère personnel, le responsable du traitement notifie la violation en question à l'autorité de contrôle compétente, 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.** **Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un <u>risque élevé</u> pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la <u>personne concernée</u> dans les meilleurs délais (avec plusieurs exceptions)** ○ **une policy en matière de gestion de sous-traitants** ○ **un template avec des instructions pour des dispositions contractuelles** ○ **un template avec des instructions pour l'exécution d'une simulation d'infraction** ○ **une policy en matière de contrôle et de gestion des fournisseurs** ○ **un template contenant des instructions pour contacter des fournisseurs externes qui ont accès aux données à caractère personnel** ○ **principes et règles en matière de signalement et d'assistance en cas d'infraction relative aux données à caractère personnel**	T2 2018 Premier draft fin déc. 2017 Version finale fin avr. 2018	**R: BCSS section sécurité** S: IPSS (concertation au sein du groupe de travail Sécurité de l'information) I: CPVP
○ **fixer les principes et les règles afin de réaliser un audit de sécurité dans le but de détecter les maillons les plus faibles et de proposer des actions concrètes aux décideurs politiques.** **À élaborer en même temps que les dispositions contractuelles relatives aux sous-traitants**	T2 2018 Version finale fin mai 2018	**R: BCSS section Sécurité & IPSS (répartition des tâches au sein du groupe de travail Sécurité de l'information)**
Pour mémoire: ○ **le cas échéant, rédiger un code de bonne conduite**	T2 2018 À évaluer	**R: BCSS section Sécurité & IPSS (répartition des tâches dans groupe travail Sécurité de l'information)**

POINT D'ACTION 4: mesures spécifiques à prendre par toute institution des secteurs social et de la santé

CONTEXTE ET OBJECTIFS:

- en concertation avec le DPO, mettre au point/élaborer/adapter ensemble de mesures afin de pouvoir appliquer la nouvelle réglementation dans les délais et dans sa totalité dans chaque institution concernée

ACTIONS ET TIMING:

Actions	Timing	Responsable
○ rendre les traitements en cours conforme à la GDPR	T1 2018	**R: IPSS**
○ **préparer une policy permettant de prouver qu'il est satisfait aux standards requis (responsabilité)** **le responsable du traitement est responsable de la conformité aux principes de la GDPR et doit aussi prouver cette conformité**	T1 2018 Premier draft fin déc. 2016 Version finale fin déc. 2017	**R: IPSS (concertation au sein du groupe de travail Sécurité de l'information)** S: BCSS section sécurité
○ implémenter la documentation/le registre (inventaire de données à caractère personnel dans les processus et inventaire des analyses d'impact relatives à la protection des données), qui peut être demandée par l'autorité de contrôle	T1 2018	**R: IPSS/BCSS**
○ préparer une culture de processus intégrant des mesures politiques internes qui satisfont aux principes de la protection des données à caractère personnel (" privacy by design") prendre des mesures techniques et organisationnelles appropriées compte tenu de la nature et des risques du traitement et uniquement traiter les données à caractère personnel qui sont nécessaires pour les finalités; ces mesures pourraient entre autres consister à réduire à un minimum le traitement des données à caractère personnel, pseudonymiser les données à caractère personnel dès que possible, garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, permettre à la personne concernée de contrôler le traitement des données et permettre au responsable du traitement de mettre en place des dispositifs de sécurité et de les améliorer	T1 2018	**R: IPSS/BCSS**
○ documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier	T2 2018	**R: IPSS/BCSS**
○ désignation d'un coordinateur responsable pour le traitement de données à caractère personnel (DPO) - continuité	T2 2018	**R: IPSS/BCSS**

point d'action 5: politique de communication avec les intéressés

EU GDPR Roadmap Belgium

CONTEXTE ET OBJECTIFS

- le fait que des données les concernant sont collectées, utilisées, consultées ou traitées doit être transparent pour les citoyens. Le principe de transparence requiert que l'ensemble des informations ou des communications relatives à un traitement de données soient aisément accessibles et faciles à comprendre. Il y a donc lieu d'utiliser des termes simples et précis. Cela concerne en particulier les informations communiquées concernant l'identité du responsable du traitement et les finalités du traitement. Il s'agit aussi des informations supplémentaires susceptibles d'être communiquées de sorte à garantir un traitement transparent et légitime;
- les citoyens doivent être informés des risques, des règles, des garanties et des droits liés au traitement ainsi que du mode d'exercice de leurs droits.

ACTIONS ET TIMING

Actions	**Timing**	**Responsable**
○ **Examen de l'impact et définition de la méthodologie** (compte tenu des exceptions du règlement et des exceptions légales supplémentaires éventuelles; voir les points d'action 1 et 2) renforcement des droits de l'intéressé (droit d'information et d'accès, droit de rectification et de suppression des données, droit de limitation du traitement, droit de portabilité des données, droit d'opposition)	T4 2017	**R: IPSS (cas par cas)**
○ préparation d'une policy pour la communication avec les intéressés une communication d'informations plus complète et une obligation de notification ainsi que des délais modifiés distinction en fonction qu'il s'agit d'une collecte directe/indirecte et cas de dispense d'informations ou communication d'informations collectives	T1 2018	**R: IPSS (cas par cas)**
○ détermination des informations et des procédures icônes normalisées	T4 2018	**R: actes délégués Commission européenne** I: CPVP, BCSS & IPSS

EU GDPR Roadmap Belgium

point d'action 6: adaptation réponses / formulaires / contrats

CONTEXTE ET OBJECTIFS:

- adapter les réponses, formulaires, contracts actuels aux nouvelles dispositions de la GDPR

ACTIONS ET TIMING:

Actions	**Timing**	**Responsable**
○ adaptation des réponses-type aux citoyens	T2 2018	**R: IPSS (cas par cas)**
○ formulaire de plainte en ligne	T2 2018	**R: CBPL** I: BCSS & IPSS
○ proposition ou approbation dispositions du contrat-type entre le responsable du traitement et le sous-traitant (art. 28.3 Règlement)	T2 2018	**R: IPSS**