FEB
Fédération des Entreprises de Belgique

CYBER SECURITY COALITION.be

DATA PROTECTION

Le nouveau règlement sur la protection des données et ses conséquences pour les entreprises en Belgique

- Nouvelles dispositions applicables à partir du **25 mai 2018**
- **Impact** sur toutes les entreprises installées dans l'espace européen
- **Sanctions** importantes en cas de non-respect

POURQUOI CETTE BROCHURE ?

Dans un monde interconnecté où les données personnelles circulent de plus en plus vite et en nombre sans cesse croissant, la protection des données et de la vie privée des personnes concernées par elles prend toute son importance.
Il s'agit là d'un nouveau paramètre incontournable pour toute entreprise qui gère un ou plusieurs fichiers de données.

Un nouveau Règlement européen vient renforcer les obligations des entreprises. Étant donné sa complexité, la FEB a conçu ce guide pratique pour comprendre les enjeux de la protection des données, prendre rapidement les mesures adéquates à mettre en œuvre et avoir les bons réflexes.

LE GDPR EST L'AFFAIRE DE TOUS !

Le GDPR entrera en vigueur le 25 mai prochain. Que cela signifie-t-il concrètement ? Toute entreprise ou organisation qui conserve ou utilise des données à caractère personnel (de son propre personnel, du personnel de fournisseurs, de clients, de prospects, etc.) devra être en mesure de prouver qu'elle le fait dans le respect des règles du GDPR.

Se conformer au GDPR n'est pas une chose qui se règle du jour au lendemain. Par ailleurs, cela requiert non seulement une connaissance approfondie de ce règlement, mais aussi de son entreprise ou organisation.

La Cyber Security Coalition entend mettre les entreprises et organisations sur la bonne voie au moyen de quelques outils. Cette brochure permet d'avoir une bonne connaissance de base du GDPR. La Coalition propose en outre un 'GDPR checkUp' pour leur permettre d'évaluer aisément elles-mêmes les démarches à entreprendre pour se mettre en ordre d'ici au 25 mai 2018.

Le 'GDPR checkUp' peut être consulté sur :
www.cybersecuritycoalition.be.

EST-CE QUE JE TRAITE DES DONNÉES PERSONNELLES ?

Traiter = collecter, enregistrer, organiser, modifier, utiliser, effacer... des données

+

Données personnelles = toute information qui se rapporte à une personne physique identifiée ou identifiable (nom, numéro national, identifiant en ligne...) appelée personne concernée

Je **traite** des données personnelles et je dois donc être **en conformité** avec la législation 'Vie privée'(*)

(*) Pour plus d'info sur le nouveau Règlement européen (EU) 2016/679 du 27 Avril 2016, voir le site de la Commission de la protection de la vie privée **www.privacycommission.be/fr**

Je suis **responsable du traitement** : je définis moi-même les finalités et la raison d'être du traitement ainsi que les moyens

Je suis **sous-traitant** : j'agis pour le compte du responsable du traitement des données

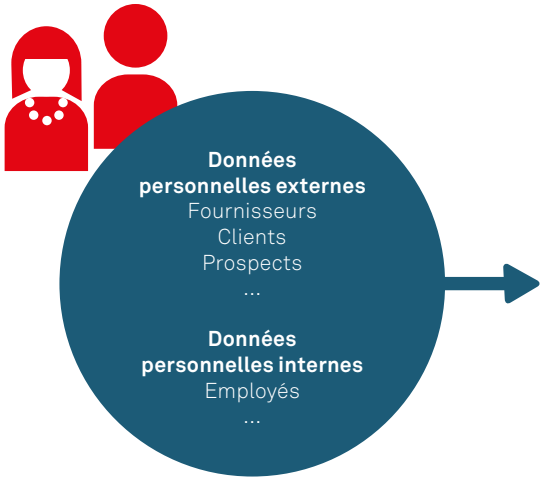
AFIN D'ÊTRE **EN CONFORMITÉ** AVEC MES OBLIGATIONS LÉGALES, JE VEILLE À CE QUE LES DONNÉES PERSONNELLES SOIENT :

- traitées **de manière légale, transparente** et que **leur utilisation soit facile à comprendre** pour la personne concernée
- **pertinentes et limitées** à l'objectif poursuivi
- collectées dans un **but déterminé, explicite et légal**
- exactes et **tenues à jour**
- conservées uniquement durant le **délai nécessaire** au traitement poursuivi
- et traitées en prenant des **mesures de sécurité informatique adéquates**

JE DOIS POUVOIR **DÉMONTRER LA CONFORMITÉ** DE MES ACTIVITÉS DE TRAITEMENT AVEC LE RÈGLEMENT. POUR CELA :

- **Je crée un registre de données** pour toutes les activités impliquant le traitement de données personnelles (inventaire)
- Je m'assure de ne traiter que **le minimum** de données personnelles nécessaires pour atteindre les objectifs de traitement légaux
- Je rédige une **privacy notice**, document d'information à communiquer aux personnes concernées qui décrit comment mon entreprise collecte, utilise, conserve,... leurs données personnelles
- **J'élabore une politique interne (internal policy)** d'information et de formation des employés
- Je désigne un employé responsable de la protection des données
- Le cas échéant, j'effectue **l'analyse d'impact relative à la protection des données**. Cette analyse me permet d'identifier les risques liés au traitement des données et la manière de les atténuer et assurer la protection de ces données
- Je mets en place des **procédures efficaces** pour assurer le respect de la législation 'vie privée'

QUELS SONT LES CAS DANS LESQUELS JE PEUX TRAITER DES DONNÉES PERSONNELLES ?



SOIT LE TRAITEMENT EST EFFECTUÉ AVEC LE CONSENTEMENT DE LA PERSONNE CONCERNÉE.

SOIT LE TRAITEMENT EST NÉCESSAIRE :

à **l'exécution d'un contrat** (ex. traitement de l'adresse de la personne concernée afin que les marchandises achetées en ligne puissent être livrées ; traitement des données de la carte de crédit afin d'effectuer le paiement)

à **l'exécution d'obligations légales** (ex. les employeurs doivent déclarer les données salariales de leurs employés à la sécurité sociale ; les autorités fiscales, les institutions financières sont tenues de déclarer certaines opérations suspectes ...)

pour protéger des **intérêts vitaux** de la personne concernée ou d'une autre personne

à l'exécution d'une tâche effectuée dans **l'intérêt public** ou dans l'exercice de l'autorité publique confiée au responsable du traitement

dans **l'intérêt légitime** (ex. une entreprise doit assurer la santé et la sécurité de son personnel travaillant dans sa centrale nucléaire en traitant certaines données notamment relatives à la santé)

Le **consentement** exige une **action affirmative claire**. Le silence, les cases pré-cochées ou l'absence de réaction ne constituent pas un consentement ! Le consentement doit être vérifiable. Cela signifie qu'il faut conserver une preuve concernant la façon et le moment où le consentement a été donné. Les individus ont le droit de **retirer leur consentement** à tout moment

DONNÉES PERSONNELLES CONCERNANT LES ENFANTS

Le General Data Protection Regulation (GDPR) contient de nouvelles dispositions visant à renforcer la protection des données personnelles des enfants

LES CONSENTEMENTS DÉJÀ OBTENUS

Je ne suis pas tenu d'obtenir un nouveau consentement des personnes concernées si celui donné auparavant répond déjà aux nouvelles exigences. Je dois donc m'assurer que ce dernier réponde bien aux normes requises par la nouvelle législation

- ○ Je veille à ce que les personnes concernées reçoivent une explication claire du traitement auquel elles consentent
- ○ Je veille à ce que le mécanisme de consentement soit vraiment volontaire et « *opt-in* »
- ○ Je m'assure que les personnes concernées puissent retirer leur consentement facilement
- ○ Je ne me fie pas au silence ou à l'absence de réaction pour considérer qu'il y a consentement

QU'EST-CE QUE LA PERSONNE CONCERNÉE PEUT ME DEMANDER ?

DÉCISION INDIVIDUELLE AUTOMATISÉE & PROFILAGE

Toute personne a le droit de ne pas être soumise à une décision individuelle lorsqu'elle est fondée exclusivement sur un traitement automatisé

Dans le cas d'une décision automatisée, je dois m'assurer que la personne peut (1) obtenir une intervention humaine dans la prise de décision ; (2) exprimer leur point de vue ; et (3) obtenir une explication de la décision et la contester

Ce droit ne s'applique pas si la décision est nécessaire pour (1) la conclusion ou l'exécution d'un contrat ou (2) est autorisée par la loi ou (3) prise sur base d'un consentement explicite

DROIT À L'OUBLI

La personne concernée peut me demander d'être « oubliée » mais ce droit n'est pas absolu

Les individus ont le droit de faire effacer leurs données personnelles et d'empêcher leur traitement si le traitement leur cause des dommages

Il existe des circonstances particulières où je peux refuser d'effacer des données personnelles

DROIT À L'INFORMATION

Je dois fournir en toute transparence des informations aux personnes concernées sur la façon dont je traite leurs données personnelles et quelles données je traite (Privacy notice)

Les informations à fournir dépendent de la manière (directe ou indirecte) dont j'ai obtenu les données personnelles

Je dois fournir les informations au moment où les données sont obtenues (si obtenues directement auprès de la personne) ou dans un délai raisonnable (obtenues indirectement)

DROIT DE RECTIFICATION

A la demande de la personne concernée, je dois :

Rectifier des données personnelles si elles sont inexactes ou incomplètes

Informer les tiers si je leur ai communiqué les données personnelles

Informer les personnes au sujet des tiers auxquels les données ont été divulguées

Répondre à la personne concernée dans un délai d'un mois (prolongeable de deux mois)

DROIT À LA PORTABILITÉ DES DONNÉES

La personne concernée peut me demander de transférer des données personnelles d'un environnement informatique à un autre d'une manière sûre et sécurisée

Seules les données personnelles qu'un individu a fournies à un responsable de traitement (sur la base du consentement ou du contrat) sont concernées

Je dois fournir les données sous une forme structurée, couramment utilisée et lisible.

Je dois le faire gratuitement et dans un délai d'un mois (prolongeable de deux mois)

DROIT D'ACCÈS

Lorsque la personne concernée en fait la demande, je dois lui fournir ses données personnelles de manière :

01 - concise, transparente, intelligible et facilement accessible, rédigée en langage clair et facile

02 - gratuitement

03 - dans un délai d'un mois (prolongeable de deux mois)

DROIT D'OPPOSITION

La personne concernée peut s'opposer :

01 - au direct marketing : lorsque je reçois une demande d'opposition, je dois cesser de traiter immédiatement les données de la personne concernée sans exceptions

02 - au traitement sur base des intérêts légitimes : lorsque je reçois une opposition, je dois arrêter le traitement de ces données sauf s'il y a des exceptions légales

03 - au traitement pour des recherches scientifiques / historiques dans certains cas. Je dois informer la personne concernée de son droit de s'opposer dès la première communication et dans la privacy notice

QUELLES SONT MES OBLIGATIONS EN TANT QUE RESPONSABLE DE TRAITEMENT OU SOUS-TRAITANT ?

Quand je traite des données personnelles, je le fais en tant que responsable de traitement ou en tant que sous-traitant.

Dorénavant, des obligations pèsent sur l'un et l'autre, alors que l'ancienne législation n'en imposait qu'au responsable de traitement !

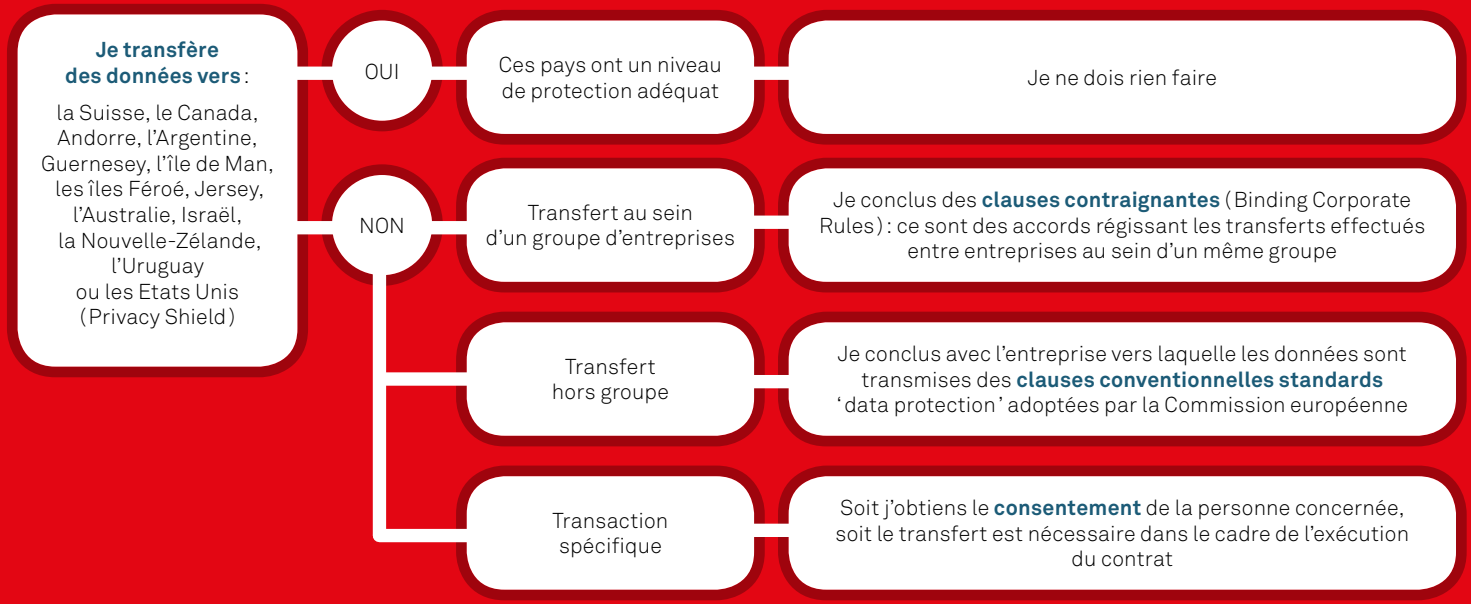
EN TANT QUE RESPONSABLE DE TRAITEMENT, JE DOIS :

- examiner toutes mes activités de traitement des données et conserver un registre d'inventaire
- m'assurer que j'ai mis en œuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité nécessaire des données à caractère personnel
- respecter le principe de responsabilisation et coopérer avec la Commission de la protection de la vie privée le cas échéant
- m'assurer que je dispose de procédures et de modèles appropriés pour identifier, examiner et signaler rapidement des violations de données à la Commission de la protection de la vie privée

EN TANT QUE SOUS-TRAITANT, JE DOIS :

- examiner mes contrats de traitement de données existants et m'assurer de la sécurité et de la confidentialité nécessaires des données personnelles que je traite
- traiter uniquement les données conformément aux instructions du responsable de traitement
- m'assurer que je dispose de procédures et de modèles appropriés pour identifier, examiner et (dans la mesure nécessaire) signaler rapidement les violations de données au responsable de traitement concerné
- noter que je ne peux désigner des sous-sous-traitants qu'avec l'autorisation du responsable de traitement

QUE DOIS-JE FAIRE SI JE TRANSFÈRE DES DONNÉES EN DEHORS L'UE ?



QUID EN CAS DE VIOLATION DE DONNÉES (DATA BREACH) ?

Violation de données à caractère personnel = destruction, perte, altération, divulgation non autorisée de données à caractère personnel

Si la violation risque de porter atteinte aux droits et libertés des individus, je dois la notifier à la Commission de la protection de la vie privée dans les 72 heures qui suivent le moment du constat. Lorsqu'une violation est susceptible d'entraîner un risque élevé pour les droits et libertés des individus, je dois en informer directement les personnes concernées

- Je m'assure que mes employés ou responsables comprennent ce qui constitue une violation des données
- Je désigne une personne chargée d'examiner et de signaler les violations de données
- Je mets en place des procédures solides de détection des infractions, d'enquête et de rapports internes
- Je prépare des lettres types afin de signaler une violation le plus rapidement possible

PERSONNE RESPONSABLE DE LA PROTECTION DES DONNÉES & DATA PROTECTION OFFICER

LA FEB CONSEILLE À TOUTES LES ENTREPRISES DE DÉSIGNER UNE PERSONNE RESPONSABLE

Lorsque votre activité principale consiste dans le traitement à large échelle et le monitoring systématique des individus ou des catégories particulières de données, vous êtes obligé de désigner un Data Protection Officer (DPO)

LES MISSIONS DU DPO

Informer et conseiller l'entreprise et ses employés sur leurs obligations de se conformer au GDPR et autres lois de protection des données

Surveiller la conformité au GDPR

Être le premier point de contact

Vous pouvez attribuer le rôle de DPO à un employé si ses fonctions professionnelles sont compatibles avec les tâches du DPO et ne conduisent pas à un conflit d'intérêts

Vous pouvez également vous adresser à un DPO externe à l'entreprise

COLOPHON

Rédaction
Nathalie Ragheno

Editeur responsable
FEB asbl
Stefan Maes
Rue Ravenstein 4
B - 1000 Bruxelles
www.feb.be

Design et mise en page
manythink

Impression
Graphius

Dépôt légal
D/0140/2016/16

Deze brochure
is ook verkrijgbaar
in het Nederlands

7 RECOMMANDATIONS INCONTOURNABLES

1. Je fais un inventaire de tous les traitements et des données traitées ainsi que de leurs objectifs
2. Je traite les données enregistrées de manière loyale et transparente
3. J'enregistre uniquement les données nécessaires et ne les conserve pas au-delà de la période utile
4. Je prends les mesures adéquates de protection des traitements et des données
5. J'informe clairement les personnes concernées par les données
6. Je mets en place une politique de protection des données et de la vie privée en interne
7. Je désigne une personne responsable de la protection des données et de la vie privée

CENTRE FOR CYBER SECURITY BELGIUM

BNP PARIBAS FORTIS

ING

KBC

proximus

SWIFT

FEB
Fédération des Entreprises de Belgique

Rue Ravenstein 4 - 1000 Bruxelles
T: + 32 2 515 08 11
info@vbo-feb.be
www.feb.be

Facebook VBO-FEB
Twitter @VBOFEB
LinkedIn VBO-FEB