Qu’est-ce le GDPR ?

GDPR, ou General Data Protection Regulation, signifie en français « RGPD » : Règlement Général sur la Protection des Données. Cette nouvelle législation a vu le jour parce que la Communauté européenne prend au sérieux la protection de ses citoyens.

Il y a actuellement, dans la Communauté européenne, différentes législations nationales en matière de protection des données personnelles. Mais, compte tenu de l’accroissement du commerce international et des échanges de données qui l’accompagnent, il est de plus en plus nécessaire de procéder à une harmonisation globale de l’ensemble des législations nationales.

Le GDPR entrera en vigueur le 25 mai 2018. Cela signifie qu’à partir de ce moment-là il y aura 1 seule nouvelle législation unifiée relative au traitement des données dans l’UE. Le non-respect du GDPR peut entraîner des sanctions !

Nous énumérons quelques-unes des raisons pour lesquelles cette législation a vu le jour :

Nouvelles technologies

Parce qu’aujourd’hui nous partageons tout avec tout le monde, nous laissons parfois des traces de nos données personnelles sans le savoir : ce que vous faites, qui sont vos amis, quelles photos vous partagiez, etc. D’autres n’ont tout simplement pas le droit d’utiliser ces données.

A partir du 25 mai, le GDPR offrira donc une meilleure protection contre la collecte et l’analyse massives de données.

Durcissement des conditions du traitement des données à caractère personnel par les organisations

Le traitement des données à caractère personnel par les organisations devient également plus strict. L’utilisation des données à caractère personnel est soumise à certaines conditions.

A partir du 25 mai, le citoyen aura donc davantage de contrôle sur le traitement de ses données à caractère personnel par des entreprises.

Que sont les données à caractère personnel ?

‘Toute information permettant d’identifier une personne …’, il peut s’agir par exemple de :

* votre numéro de registre national
* votre nom
* votre adresse
* votre photo
* votre adresse e-mail
* votre numéro de telephone
* etc.

Au nombre des données à caractère non personnel figurent par exemple :

* la marque lyreco,
* le nombre d’habitants en Belgique
* ou encore les statistiques globales relatives aux personnes handicapées
* etc.

Qui joue un rôle dans le GDPR ?

1. **Les ‘personnes concernées’**, appelées les personnes concernées, qui sont identifiées ou identifiables et à propos desquelles des données sont traitées. Il s’agit de tout citoyen de l’UE. On donne souvent à la personne concernée un autre nom, celui de ‘data subject’ ;
2. **Le ‘responsable du traitement’**, ou controller, fixe l’objectif et les moyens du traitement des données à caractère personnel ;
3. Enfin, c’est pour celui-ci que **le ‘sous-traitant’**, ou « processor », traite les données à caractère personnel.

A quels traitements le RGPD est-il applicable ?

Le traitement de données à caractère personnel de personnes concernées, également en cas de traitement automatisé partiel, par une entreprise ou une organisation établie dans l’Union européenne. Le traitement proprement dit dans l’Union n’a pas d’importance.

Par exemple : un siège européen d’une multinationale, mais le traitement proprement dit est externalisé en Inde; le RGDP est applicable.

La législation du RGPD est applicable à toutes les entreprises (également non européennes) qui traitent des données à caractère personnel de personnes concernées dans l’Union européenne, dans le cadre de l’offre de biens ou de services (contre paiement ou non) ou dans le cadre du monitoring du comportement des intéressés.

Par exemple : une entreprise qui a un siège dans l’UE offre à des clients résidant dans les Etats baltes des produits de voyages et traite dans ce cadre des données à caractère personnel de personnes physiques.

A quels traitements le RGPD n’est-il PAS applicable ?

Les règles ne sont pas applicables au traitement de données par un individu pour des raisons purement personnelles ou pour des activités qui ont lieu au domicile d’une personne, à condition qu’il n’y ait pas de lien avec une activité professionnelle ou commerciale.

Par exemple quelqu’un utilise son carnet d’adresses personnel pour inviter des amis par e-mail à une fête qu’il ou elle organise (exception domestique).

Et le RGPD n’est également pas applicable aux traitements par des autorités compétentes en vue de prévenir, de détecter ou de poursuivre des faits délictueux, aux enquêtes en la matière ou à l’exécution de peines, y compris la protection et la prévention contre les dangers pour la sécurité publique. Ceci dans le cadre d’activités qui sortent du champ d’application du droit de l’Union.

Qui est responsable du respect du RGPD ?

Toute institution publique (et également la plupart des institutions privées) est obligée de désigner un **DPO, à savoir un ‘data protection officer’**. Il formule des avis, il informe et il contrôle la protection des données et de la vie privée.

**L’APD, à savoir l’Autorité de protection des données**, remplace l’actuelle Commission de la protection de la vie privée. Elle émet des avis et contrôle la protection des données et de la vie privée, elle inflige des sanctions lorsque des données sont traitées d’une manière non conforme à la législation RGPD.

Elle se concerte avec **le Comité européen de la protection des données** et collabore avec d’autres APD. Le Comité européen de la protection des données est compétent au niveau européen et a également des attributions en matière de contrôles et de sanctions.

Quelle est l’interaction entre toutes les parties concernées ?

**Le responsable du traitement ou controller** informe l’intéressé au sujet du traitement. Le responsable du traitement peut à cet effet éventuellement faire appel à **une personne chargée du traitement (à savoir le processor)**.

Ces deux personnes peuvent demander l’avis de **leur DPO, à savoir le data protection officer**.

**Le responsable du traitement ou l’intéressé** peuvent tous deux **demander des informations ou des avis à l’Autorité de protection des données (APD)**.

L’Autorité de protection des données (APD) **collabore avec le Comité européen de la protection des données**, effectue entre autres des contrôles auprès du responsable du traitement et peut également communiquer des informations aux intéressés.

L’APD collabore parfois aussi avec d’autres APD d’autres pays.

Façons de traiter les données à caractère personnel

Les données à caractère personnel peuvent être traitées de multiples façons, par exemple : collecte, consultation, stockage, enregistrement, classement, modification, demande, effacement, transmission, etc. Et ainsi de suite !

Dans notre SPF, nous traitons aussi souvent des données à caractère personnel : citons à titre d’exemples

* le paiement des salaires,
* la création de dossiers,
* la capture d'un événement en photos,
* l’établissement d’un classement,
* la clôture de dossiers,
* la modification de données,
* la création d'abonnements de collaborateurs,
* la consultation de l'agenda de collègues,
* la numérisation de documents,
* le traitement de commandes.

Principes plus stricts en matière de protection de donnnées

Bon nombre de ces principes de protection des données existent depuis longtemps en droit belge, mais dans le GDPR, ils sont encore bien plus stricts. Un grand nombre de ces principes ont trait à l’exactitude de la documentation et à la licéité des actes. Nous les répertorions pour vous :

* **Transparence et légitimité :** la personne dont les données sont traitées en a connaissance et connaît ses droits.
* **Finalité déterminée :** les données à caractère personnel ne peuvent être collectées et utilisées qu'à des fins légitimes.
* **Limitation à ce qui est nécessaire (ou minimisation) :** seules les données nécessaires à la réalisation de l'objectif visé peuvent être collectées.
* **Exactitude :** les données à caractère personnel doivent être correctes et tenues à jour.
* **Limitation de conservation ou de stockage :** les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées.
* **Intégrité et confidentialité :** les données personnelles doivent être protégées contre tout accès non autorisé, perte ou destruction.
* Ce qui est nouveau, c'est **l’obligation de responsabilité** des organisations et des entreprises : le contrôleur doit être en mesure de démontrer qu’il respecte les règles.

En vertu de quelle légitimité traitons-nous des données personnelles ?

Afin d'être autorisé à traiter des données personnelles, il faut disposer d’une base juridique, d’une légitimité.

Nous exposons ici quelques possibilités :

* La première = le **consentement explicite de la personne concernée** ; c'est-à-dire qu'un citoyen de l'UE donne son consentement pour quelque chose, mais qu'il peut aussi le retirer.
* La seconde = lorsque **cela est nécessaire pour exécuter un contrat** ; par exemple, pour traiter l'adresse de quelqu'un qui a commandé quelque chose en ligne, ou pour traiter les données d’une carte de crédit pour traiter un paiement.
* La troisième = afin de se conformer **à une obligation légale ; c’est le cas pour l’essentiel du traitement des données personnelles exécuté dans notre SPF** - Par exemple : les employeurs doivent transmettre à la sécurité sociale des données relatives aux travailleurs, ou il suffit de penser à la législation portant sur toutes sortes de mesures de soutien pour les personnes handicapées, ou à la Commission Artistes, ....
* La quatrième = pour protéger les **intérêts vitaux** d'une personne concernée ; on ne peut recourir à cette possibilité que s'il est nécessaire d'utiliser des données pour sauver la vie de quelqu’un.
* La cinquième = pour l'exécution d'une mission **d'intérêt général** ; c'est par exemple plutôt le cas pour le traitement de données par la police).
* Enfin, la sixième = pour la défense **d'un intérêt légitime** ; par exemple une entreprise du secteur nucléaire a un intérêt légitime à traiter certaines données personnelles spécifiques de son personnel afin de pouvoir garantir la sécurité et la santé de ce personnel.

Droits et obligations

Les personnes concernées, ou les citoyens de l'UE, ont des droits. Les organisations et les entreprises (et donc les responsables du traitement et les sous-traitants) ont des obligations à leur égard.

**Premièrement, il y a le droit à l'information**. Cela signifie que toute personne concernée a le droit d'être informée :

* des données qui sont collectées par une entreprise ou une organisation
* de la finalité pour laquelle elles sont utilisées et du fait qu’elle soient partagées avec qui que ce soit
* du temps durant lequel elles sont conservées
* de la base (juridique) sur laquelle ces données sont collectées
* de l’amélioration de la manière dont la personne concernée peut exercer ses autres droits, tels que le droit de consulter ses données, ....

**Deuxièmement, il y a le droit d'accès :** la personne concernée peut demander l'accès aux données concrètes qu'une entreprise ou une organisation traite à son sujet (par exemple, des données concrètes dans un dossier). L'entreprise ou l'organisation est alors obligée de partager toutes les informations avec la personne concernée. Il va sans dire que l'identité du demandeur doit être vérifiée.

**Troisièmement, il y a le droit de rectification :** une personne a le droit de demander que ses données soient corrigées.

**Quatrièmement, il y a le droit d'être oublié** (ce qui n'est pas tant le cas pour notre SFP). Toute personne a le droit, sous certaines conditions, d'exiger la suppression des données personnelles détenues par une entreprise ou une organisation. D'autres lois qui obligent la société ou l'organisation à conserver certaines données ont préséance sur cette règle.

**Cinquièmement, il y a le droit d'opposition :** les personnes concernées peuvent demander l’arrêt du traitement, par exemple jusqu'à ce que leurs données erronées aient été corrigées.

**Sixièmement, il y a le droit à la transférabilité** (ce qui n'est pas tant le cas non plus pour notre SFP). Si la personne concernée demande que le traitement des données soit effectué par une autre organisation. Il suffit de penser à des exemples comme Spotify (une base de données musicales), si la personne concernée veut que les données soient transférées vers Soundcloud (une autre base de données musicales).

**Et enfin, septièmement, il y a le droit en matière de prise de décision automatisée et de profilage** (non applicable au sein de notre SFP). Les personnes concernées peuvent demander qu’il y ait au moins une intervention humaine dans le traitement, qu’il ne soit pas entièrement automatisé.
Les organisations et les entreprises ont des obligations envers les personnes concernées, ce qui signifie qu'elles ont une obligation de responsabilité (accountability). En tant que SFP, nous devons donc, nous aussi, être en mesure de soumettre des preuves à l'APD (Autorité de protection des données) concernant toutes les données personnelles que nous traitons. Ce sont des choses que nous aussi, dans notre SFP, devons documenter correctement …

Obligations des organisations et entreprises

Il s’agit dans ce cadre de toutes sortes d'actions, telles que

* la création d'un inventaire du traitement des données à caractère personnel (en ce compris toutes les informations relatives à la finalité, etc.)
* la rédaction d'une déclaration de confidentialité, dans laquelle notre traitement des données est expliqué dans un langage simple et dans laquelle plus d'informations sont données sur les droits des personnes concernées.
* la formation du personnel (information et sensibilisation)
* la désignation d'un DPD (délégué à la protection des données)
* l’exécution d’analyses d'impact : lors du traitement de données à caractère personnel présentant des risques plus élevés, lorsque la protection semble insuffisante, nous devons en informer l'APD (ou l'autorité de protection).
* l’élaboration de procédures en matière de sécurité de l'information et de surveillance de la protection de la vie privée.
* si nous travaillons avec des sous-traitants externes, nous devons nous assurer qu'ils travaillent également en conformité avec le RGPD.
* nous devons veiller aux 5 justifications possibles que nous avons mentionnées plus haut (par exemple : consentement, intérêt légitime, intérêts vitaux, etc.)
* enfin nous devons également élaborer des procédures à appliquer au cas où des problèmes se produiraient (p. ex. fuites de données).

Que signifie le GDPR pour vous

Constatez-vous des problèmes liés à des données ?

Malgré toutes les mesures de protection, des problèmes peuvent survenir au niveau des données que nous traitons, par exemple suite à des manipulations erronées, à un cambriolage, à des pannes techniques et ainsi de suite !

De ce fait, il peut y avoir des pertes ou des destructions de données. Des données peuvent être modifiées indûment et perdre ainsi leur intégrité. Ou bien des données peuvent être divulguées publiquement à des personnes non qualifiées. Chaque collaborateur doit coopérer afin d’avoir une réaction appropriée.

Que devez-vous faire en cas de problèmes ?

Il faut toujours le signaler le plus tôt possible afin de pouvoir prendre des mesures destinées à y remédier et à faire face à ses éventuelles conséquences.

Informez-en immédiatement votre responsable et le DPO (Data Protection Officer – Délégué à la protection des données ) du SPF, via DPO@minsoc.fed.be.

Communiquez-leur immédiatement toutes les informations utiles dont vous disposez à ce moment-là, ce qui facilite les recherches ultérieures et accélère la suite de l’approche.

En cas de problèmes graves, le DPO doit également informer l’APD (Autorité de protection des données) dans les 72 heures.

Quelles informations pouvez-vous par exemple déjà transmettre :

* Qu’avez-vous remarqué, que s’est-il passé, quelles données ou avec quelle application sont concernées ?
* Quand cela s’est-il produit ?
* Qui en subit les inconvénients ? Par exemple des collaborateurs de votre service, d’autres services ? Des citoyens ou des entreprises ? Des institutions partenaires ?
* Voyez-vous une cause possible au problème ?
* Avez-vous déjà pris des mesures vous-même, et si oui, lesquelles ? Avez-vous par exemple déjà informé d’autres collègues ?

Questions de citoyens ...

Comme nous l’avons déjà expliqué dans la partie 3, la personne concernée ou le citoyen a de nombreux droits et il peut donc poser des questions sur ses données à caractère personnel qui font l’objet d’un traitement. Il est donc tout à fait possible qu’ils vous adressent à vous aussi une demande !

Le citoyen peut, par exemple, demander

* quelles données sont effectivement traitées
* quels traitements sont effectués,
* pour quelles raisons,
* pendant combien de temps nous gérons ces données, avec qui elles sont échangées, etc.

Il peut en outre demander de

* faire corriger des données,
* d’être oublié
* ou de s’opposer à certains traitements

Comment répondez-vous à des questions posées par des citoyens ?

Les citoyens peuvent poser leurs questions directement au DPO (Délégué à la protection des données), mais également, bien sûr, directement à votre service ou à vous. Si des questions vous sont posées, il est préférable de les signaler immédiatement à votre responsable et au DPO.

Une demande d’accès aux données, par exemple, doit recevoir une réponse dans un délai d’un mois. Il est donc nécessaire de transmettre cette demande le plus rapidement et le plus complètement possible.

Il importe également de pouvoir vérifier l’identité du citoyen afin de s’assurer que c’est bien cette personne-là qui demande l’accès aux données.

Quelles informations pouvez-vous par exemple déjà transmettre :

* Quelle est la question posée par le citoyen ?
* Quand avez-vous reçu la question ?
* Avez-vous déjà pris vous-même des mesures ? Si oui, lesquelles ?
* Avez-vous déjà vérifié l’identité du citoyen ?

Collaborez-vous avec des partenaires externes ?

Lorsque nous concluons un accord avec un sous-traitant externe, qui traite également des données à caractère personnel en notre nom, vous devez toujours vous assurer que ce 'sous-traitant' externe travaille aussi dans le respect de la législation RGPD. A cet égard, il suffit de penser par exemple à des marchés publics ou à des contrats.

Comment concluez-vous un accord avec un sous-traitant externe ?

Si vous (ou votre DG/Service) concluez un accord avec un sous-traitant externe ou si vous vous préparez à lancer un marché public, certaines conditions doivent être remplies.

Pour ce faire, vous devez contacter le Service Marchés publics (du Service d’encadrement B&CG) et le DPO.

Transmettez toutes les informations que vous détenez sur le sous-traitant, telles que :

* De quel(s) sous-traitant(s) externe(s) s’agit-il ?
* Quelles sont les dates de début et de fin de l’accord ?
* Quelles données à caractère personnel sont traitées ou échangées ?
* Quelles sont les personnes de contact chez le sous-traitant ?

Entamer une nouvelle tâche ou un nouveau traitement au SPF

Si, dans notre SPF, nous voulons entamer une nouvelle tâche ou un nouveau traitement, il est préférable de réfléchir à l'avance aux aspects relatifs à la protection de la vie privée et aux règles du RGPD que nous devons appliquer. Ceci vaut également pour la modification d'une tâche existante, si le type de données que nous traitons ou la manière dont les données sont traitées change.

Les chefs de projet et les services concernés doivent donc toujours y penser, dès le stade de la conception et de l'organisation de la tâche.

Si nous traitons des données à caractère personnel, nous devons documenter ce fait, comme nous l'avons déjà mentionné.

Que devons-nous vérifier ?

* Allons-nous traiter des données à caractère personnel (ou les traiter autrement qu’avant) ? Si oui, lesquelles ?
* Disposons-nous d’une base juridique pour le traitement ? Si oui, de laquelle ? (par exemple un cadre légal ou le consentement de la personne concernée)
* Nous devons également nous demander quels sont les risques d’atteinte à la vie privée pour le traitement concerné, par exemple en matière de confidentialité, d’intégrité et de disponibilité continue de ces données.
* Sur la base de cette analyse des risques, nous prenons ensuite les éventuelles mesures préparatoires nécessaires pour garantir un traitement sûr (par exemple sécuriser l’accès aux données).

Dans le cas de nouveaux traitements ou de traitement modifiés, nous pensons également à l’avance à des mesures permettant de répondre de manière efficace et transparente aux questions des citoyens.

Avez-vous pensé à toutes les questions ? N’hésitez pas à contacter notre DPO car il peut vous aider et vous assister dans cette démarche.

Restez toujours attentif …

La sécurité de l'information et la surveillance de la vie privée sont l'affaire de tous. Restez donc toujours attentif et respectez en tout temps les consignes suivantes !

**Tout d’abord, prévenir les cambriolages :** assurez-vous d'avoir un mot de passe solide, et NE LE PARTAGEZ PAS ! Activez toujours l'économiseur d'écran, de manière à ce que personne ne puisse utiliser votre PC en votre absence. Signalez toujours sans délai la perte ou le vol. Attention à l'ouverture des courriels : ne vous laissez pas attraper par des courriels de phishing. Faites attention à la navigation sur Internet et protégez votre smartphone.

**Deuxièmement, évitez les fuites d'informations :** imprimez toujours des documents importants de manière sécurisée, ne laissez pas traîner des documents ! Sur les bureaux, appliquez toujours le principe du « clean desk ». Évitez de transmettre des pièces jointes par mail, stockez les documents sur nos sites sécurisés et envoyez des hyperliens à vos collègues. Évitez de transmettre des clés USB, des CD ou des DVD contenant des informations importantes. Faites également attention au transfert de données à caractère personnel par e-mail, votre e-mail peut arriver à une mauvaise adresse.

**Et, enfin, prévenez les violations de la vie privée :** ne conservez jamais dans le Cloud des informations qui sont liées à la Banque Carrefour de la Sécurité Sociale (BCSS) ou à des bases de données applicatives, prêtez attention à vos paramètres de confidentialité, par exemple sur les médias sociaux, et surfez incognito.

----------------------------

Wat is de GDPR?

GDPR, of General Data Protection Regulation, in het Nederlands ‘AVG’, Algemene verordering gegevensbescherming. Het is een nieuwe privacywetgeving die vanaf 25 mei 2018 van kracht gaat, omdat de europese gemeenschap de bescherming van zijn burgers ernstig neemt.

Nu zijn er in de EU verschillende nationale wetten rond privacy, maar door de toenemende internationale handel en het gegevensverkeer dat daarmee gepaard gaat, groeit de nood aan een overkoepelende harmonisatie, en dus een eenduidige wet in de hele EU.

Vanaf 25 mei 2018 gaat de GDPR van kracht. Dat betekent er vanaf dan 1 nieuwe, eenduidige wet voor gegevensverwerking is in de EU. Het niet naleven van de GDPR-wetgeving, kan sancties inhouden!

Redenen voor het invoeren van deze nieuwe privacywet zijn:

Nieuwe technologieën

We delen zoveel informatie via het internet dat we soms sporen achterlaten met persoonlijke gegevens zonder dat we het weten: wat je doet, wie je vrienden zijn, wat je lievelingskleur is van schoenen, de regio waar je op huizenjacht gaat, enzovoort. Anderen mogen al die gegevens niet zomaar gebruiken!

Vanaf 25 mei biedt de GDPR dus een betere bescherming tegen massale gegevensinzameling en -analyse.

Verwerking persoonsgegevens door organisaties

Ook de verwerking van persoonsgegevens door organisaties verstrengt. Er hangen voorwaarden vast aan het gebruik van persoonsgegevens.

Vanaf 25 mei is er dus meer controle voor de burger op de verwerking van zijn persoonsgegevens door bedrijven.

Wat zijn persoonsgegevens?

‘Alle informatie waarmee iemand geïdentificeerd kan worden’, zoals:

* je rijksregisternummer
* je naam
* de naam van je beste vriend
* je telefoonnummer
* je adres
* je muzikale voorkeur
* je e-mailadres
* een foto
* … enz.

Wat geen persoonsgegevens zijn, is bijvoorbeeld:

* merknamen, bijvoorbeeld het merk “Lyreco”
* het aantal inwoners van België
* globale statistieken, bijvoorbeeld over personen met een handicap
* … enz.

Deze informatie moet opgenomen worden in een privacyverklaring.

Wie zijn de actoren, of wie speelt er allemaal een rol bij de GDPR?

1. **De ‘betrokkene’**, of elke natuurlijke persoon, burger in de EU, geïdentificeerd of identificeerbaar, over wie gegevens verwerkt worden. Een veel gebruikte term is ook ‘data subject’).
2. **De ‘verwerkingsverantwoordelijke’**, of controller, stelt vast wat het doel is van en de middelen voor de verwerking van persoonsgegevens.
3. **De ‘verwerker’**, of processor, verwerkt de persoonsgegevens voor de verwerkingsverantwoordelijke.

Welke gegevensverwerkingen vallen onder de GDPR?

De verwerking van persoonsgegevens van burgers in de Europese Unie door een bedrijf of organisatie gevestigd in de EU, ook als het slechts om een gedeeltelijk geautomatiseerde verwerking gaat. Het is niet van belang dat de verwerking zelf in de EU gebeurt.

Bijvoorbeeld: wanneer een Europese multinational persoonsgegevens van EU burgers verwerkt, maar die verwerking uitbesteedt aan India, valt dit ook onder de GDPR.

De GDPR-wetgeving is ook van toepassing op alle organisaties en bedrijven (ook niet-¬Europese) die persoonsgegevens verwerken van burgers uit de Europese Unie, bij het aanbieden van goederen of diensten (betalend of niet) of in het kader van de monitoring van gedrag.

Bijvoorbeeld: een onderneming met een vestiging in de EU biedt klanten die in de Baltische staten wonen reisproducten aan en verwerkt dus persoonsgegevens.

Welke gegevensverwerkingen vallen NIET onder de GDPR?

De GDPR is niet van toepassing op de verwerking van gegevens door een individu voor louter persoonlijke redenen of ten behoeve van activiteiten die bij iemand thuis plaatsvinden, mits er geen link is met een beroeps- of handelsactiviteit.

Bijvoorbeeld: iemand gebruikt zijn of haar persoonlijk adressenboekje om vrienden via e mail uit te nodigen voor een door hem of haar georganiseerd feest.

Deze regel is ook niet van toepassing voor verwerkingen door de bevoegde autoriteiten met het oog op de voorkoming, de opsporing en de vervolging van strafbare feiten, het onderzoek errond of de uitvoering van straffen. Daarbij hoort ook de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Wie is verantwoordelijk voor de naleving?

Alle overheidsinstellingen (en ook de meeste private instellingen) worden verplicht om een **DPO of ‘data protection officer’** aan te duiden. Hij adviseert, informeert en controleert de gegevensbescherming en privacybewaking van zijn organisatie.

De **GBA of Gegevensbescherming Autoriteit** vervangt de huidige Privacy Commissie. Deze adviseert en controleert de gegevensbescherming en privacybewaking, hij sanctioneert wanneer gegevens niet conform de GDPR-wetgeving verwerkt worden.

Hij overlegt met **het Europees comité voor gegevensbescherming** en werkt samen met andere GBA’s. Het Europees Comité voor Gegevensbescherming is bevoegd op Europees vlak, en heeft ook een controlerende en sanctionerende bevoegdheid.

Wat is de wisselwerking tussen de verschillende actoren?

**De verwerkingsverantwoordelijke of controller** informeert de betrokkene over de verwerking. Hij/zij kan daarvoor eventueel **beroep doen op een verwerker (of processor)**. Beide kunnen beroep doen op **advies van hun DPO of data protection officer**.

De verwerkingsverantwoordelijke of de betrokkene kunnen beide informatie en **advies vragen** aan de **gegevensbeschermingsautoriteit (GBA)**. De GBA **werkt samen met het Europees comité voor gegevensbescherming**, voert onder andere controles uit bij de verwerkingsverantwoordelijke en kan ook informatie verstrekken aan de betrokkenen.

Soms **werkt** de GBA **ook samen** met andere **GBA van andere landen**.

Hoe kan je persoonsgegevens verwerken?

Persoonsgegevens kan je op ontelbare manieren verwerken, bijvoorbeeld: verzamelen, raadplegen, opslaan, vastleggen, ordenen, wijzigen, opvragen, verwijderen, doorgeven, …. En ga zo maar door!

Bij onze FOD verwerken we ook vaak persoonsgegevens, enkele voorbeelden:

* lonen uitbetalen,
* dossiers aanmaken,
* een evenement op foto vastleggen,
* een klassement aanleggen,
* dossiers afsluiten,
* gegevens wijzigen,
* werknemersabonnementen aanmaken,
* de agenda van je collega raadplegen,
* documenten inscannen,
* bestellingen behandelen.

Verstrenging principes gegevensbescherming

Veel van die principes rond gegevensbescherming bestaan al lang in de Belgische wetgeving, maar in de GDPR worden deze nog aanzienlijk verstrengd.Veel van de principes hebben te maken met de juiste documentatie en rechtmatig handelen.

We zetten ze voor jou op een rij:

* **Transparantie en legitimiteit:** de persoon van wie gegevens verwerkt worden is hiervan op de hoogte, en kent zijn rechten.
* **Doelgebonden:** persoonsgegevens mogen uitsluitend voor gewettigde doeleinden verzameld en gebruikt worden.
* **Gegevensbeperking (of minimalisatie):** alleen de gegevens die nodig zijn om het beoogde doel te bereiken, mogen worden verwerkt
* **Juistheid** persoonsgegevens moeten correct zijn, en up to date gehouden worden
* **Bewaar- of opslagbeperking:** de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel
* **Integriteit en vertrouwelijkheid:** persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
* Wat nieuw is, is de **verantwoordingsplicht** voor organisaties en bedrijven: de verwerkingsverantwoordelijke moet kunnen aantonen aan de regels te voldoen.

Met welke rechtvaardiging verwerken we persoonsgegevens?

Om persoonsgegevens te mogen verwerken, moet je een rechtsgrond, een rechtvaardiging hebben.

Hierbij belichten we enkele mogelijkheden:

* De eerste = **expliciete toestemming van de betrokkene**, dat wil zeggen dat iemand voor iets zijn toestemming geeft, maar hij of zij kan die ook weer intrekken.
* De tweede = wanneer het **noodzakelijk is voor het uitvoeren van een overeenkomst**, bijvoorbeeld het verwerken van het adres van iemand die iets online bestelde, of het verwerken van kredietkaartgegevens om een betaling te verwerken.
* De derde = om te voldoen aan een **wettelijke verplichting, de verwerking van persoonsgegevens in onze FOD valt hier hoofdzakelijk onder** – Bijvoorbeeld: werkgevers moeten gegevens over werknemers doorgeven aan de sociale zekerheid, of denk maar aan wetgevingen rond allerlei steunmaatregelen voor personen met een handicap, of de Commissie Kunstenaars,…
* De vierde = om de **vitale belangen** van een betrokkene te beschermen, dus dit mag enkel gebruikt worden als er een noodzaak bestaat om gegevens te gebruiken om iemands leven te redden of te beschermen.
* De vijfde = voor het uitvoeren van een taak van **algemeen belang** (dit is bijvoorbeeld eerder voor verwerkingen van gegevens door politie).
* En tenslotte de zesde = voor de behartiging van een **gerechtvaardigd belang**, zo heeft bijvoorbeeld een onderneming in de nucleaire sector een ‘gerechtvaardigd belang’ om enkele specifieke persoonsgegevens te verwerken van haar personeel om de veiligheid en gezondheid van dat personeel te kunnen garanderen )

Rechten en plichten

Betrokkenen, of EU burgers, hebben rechten. De organisaties en bedrijven (en dus de verwerkingsverantwoordelijken en verwerkers), hebben verplichtingen tegenover hen.

Rechten van de betrokkenen

Ten eerste het recht op informatie. Dat betekent dat elke betrokkene het recht heeft om op de hoogte te zijn van:

* Welke gegevens een bedrijf of organisatie verzamelt,
* Waarvoor deze gebruikt worden en of ze met iemand gedeeld worden (en hoe je het gebruik ervan rechtvaardigt),
* Hoe lang ze bewaard worden,
* De manier waarop betrokkene gebruik kan maken van zijn andere rechten, zoals het recht om zijn data te raadplegen, te laten verbeteren, ...

**Ten tweede is er het recht op inzage**: de betrokkene mag inzage vragen in de concrete gegevens die een bedrijf of organisatie over hem verwerkt (vb: concrete dossiergegevens). Het bedrijf of de organisatie is dan verplicht alle informatie met de betrokkene te delen. Uiteraard moet men de identiteit van de aanvrager controleren.

**Ten derde is er het recht op correctie**, wat betekent dat een persoon het recht heeft om te vragen om zijn gegevens te verbeteren.

**Ten vierde is er het recht om vergeten te worden** (dit is niet zozeer van toepassing voor onze FOD). Elke persoon heeft het recht, onder bepaalde voorwaarden, te eisen dat persoonlijke data waarover een bedrijf of organisatie beschikt, gewist worden. Andere wetten die het bedrijf of de organisatie verplichten bepaalde data te bewaren gaan voor op deze regel.

**Ten vijfde is er het recht van verzet:** betrokkenen kunnen vragen om de verwerking te staken, bijvoorbeeld tot zijn foutieve gegevens zijn gecorrigeerd.

**Ten zesde is er het recht op overdraagbaarheid** (ook dit is niet zozeer van toepassing voor onze FOD). Als betrokkene zou vragen om de gegevensverwerking door een andere organisatie te laten uitvoeren. Maar denk maar aan voorbeelden zoals Spotify (een muziekdatabank), als jij je gegevens wil laten overmaken aan Soundcloud (een andere muziekdatbank).

**Ten zevende en laatste is er het recht i.v.m. geautomatiseerde besluitvorming en profilering** (niet van toepassing binnen onze FOD). Betrokkenen kunnen vragen dat er minstens toch een menselijke tussenkomst is in de verwerking, dat niet volledig geautomatiseerd is.

Plichten van bedrijven en organisaties

Organisaties en bedrijven hebben plichten tegenover de betrokkenen, zij hebben dus een verantwoordingsplicht (over accountability). Ook wij als FOD moeten dus bewijzen kunnen voorleggen aan de GBA (of beschermingsautoriteit) over alle persoonsgegevens die we verwerken. Dit zijn zaken die ook wij, bij onze FOD goed moeten documenteren….

We denken hierbij aan allerlei acties, zoals:

* Het aanmaken van een inventaris van de verwerkingen van persoonsgegevens (met daarin dus alle informatie over het doeleinde, enzovoort).
* Het opmaken van een privcayverklaring, waarin in eenvoudige taal onze gegevensverwerkingen uitgelegd worden en waarin meer informatie staat over de rechten van de betrokkenen.
* Het trainen van medewerkers (hen informeren en sensibiliseren)
* Het aanduiden van een DPO (Data protection officer)
* Impactanalyses uitvoeren wanneer we persoonsgegevens verwerken met hogere risico’s, wanneer de bescherming onvoldoende zou blijken, moeten we de GBA (of gegevensbescherminsgautoriteit) inlichten
* Procedures opstellen in verband met informatieveiligheid en privacybewaking
* Als we met externe verwerkers werken, moeten we toezien dat zij ook conform de GDPR-wetgeving werken
* We moeten toezien op de 5 mogelijke rechtvaardigingen die we eerder opnoemden (bijvoorbeeld: toestemming, gerechtvaardigd belang, vitale belangen, enzovoort)
* En ten laatste moeten ze ook procedures uitwerken voor wanneer er problemen zouden voorkomen (bijvoorbeeld datalekken).

Wat betekent de GDPR concreet voor jou?

Stel je problemen vast met gegevens?

Ondanks alle beschermingsmaatregelen kunnen er toch problemen opduiken met de gegevens die we verwerken, door verkeerde manipulaties, door inbraak, technische storingen en noem maar op! Daardoor kunnen bijvoorbeeld gegevens verloren gaan of vernietigd worden.

Gegevens kunnen onterecht gewijzigd worden en zo hun integriteit verliezen. Of gegevens kunnen publiek onthuld worden aan mensen die onbevoegd zijn. Iedere medewerker moet eraan meewerken om hier gepast op te reageren.

Wat moet je doen als je een probleem opmerkt?

Je moet dit altijd zo vlug mogelijk signaleren om acties te kunnen ondernemen om het probleem en eventuele gevolgen ervan aan te pakken.

Verwittig dus onmiddellijk je verantwoordelijke en de DPO van de FOD, via DPO@minsoc.fed.be. Geef hen meteen alle nuttige informatie mee waarover je op dat moment beschikt, dat vergemakkelijkt verdere opzoekingen en versnelt de verdere aanpak.

Bij ernstige problemen moet de DPO ook immers de (GBA) Gegevens Beschermings Autoriteit binnen de 72u inlichten.

Wat zijn voorbeelden van informatie die je al kan doorgeven:

* Wat heb je opgemerkt, of wat is er gebeurd, met welke gegevens of welke toepassing?
* Wanneer gebeurde dit?
* Wie ondervindt er nadelen van? Bijvoorbeeld medewerkers van je dienst, andere diensten? Burgers, of ondernemingen? Partnerinstellingen?
* Zie jij een mogelijke oorzaak?
* Heb je zelf al acties ondernomen, en zo ja, welke? Heb je bijvoorbeeld al andere collega’s geïnformeerd?

Vragen van burgers...

De betrokkene of burger heeft veel rechten, en hij of zij kan dus vragen stellen over persoonsgegevens die van hem of haar verwerkt worden. Het is dus goed mogelijk dat ook jij een vraag ontvangt.

De burger kan bijvoorbeeld vragen

* welke gegevens concreet verwerkt worden,
* welke verwerkingen uitgevoerd worden,
* om welke redenen,
* hoe lang we die gegevens beheren,
* met wie we ze uitwisselen enzovoort.

Daarnaast kan hij of zij ook vragen stellen om gegevens te laten aanpassen, dat kan zijn:

* gegevens laten corrigeren
* vragen om vergeten te worden
* bezwaar aantekenen tegen bepaalde verwerkingen

Hoe beantwoord je vragen van burgers?

Burgers kunnen hun vragen rechtstreeks aan de DPO (data protection officer) stellen, maar uiteraard ook rechtstreeks aan jouw dienst of aan jou. Wanneer jij vragen krijgt, signaleer je dat best onmiddellijk aan je verantwoordelijke en aan de DPO.

Een vraag om inzage in gegevens bijvoorbeeld moet binnen de maand beantwoord worden. Dit vlug en zo volledig mogelijk doorspelen is dus noodzakelijk. Belangrijk is ook dat we de identiteit van de burger kunnen controleren, om ons ervan te verzekeren dat het weldegelijk die persoon is die gegevens opvraagt.

Stel je dus zeker een paar vragen voor je contact opneemt met je verantwoordelijke en je DPO, bijvoorbeeld:

* Welke vraag stelt de burger?
* Wanneer heb je de vraag ontvangen?
* Heb je zelf al acties ondernomen? Zo ja, welke?
* Heb je de identiteit van de burger al gecontroleerd?

Werk je samen met externe personen/verwerkers?

Wanneer een medewerker van de FOD een overeenkomst afsluit met een externe verwerker, en die ook in opdracht van ons persoonsgegevens verwerkt, moet je jezelf er altijd van verzekeren dat ook die externe ‘verwerker’ conform de GDPR-wetgeving werkt. Denk daar aan bijvoorbeeld overheidsopdrachten of contracten.

Hoe sluit je een overeenkomst met een externe verwerker?

Als een medewerker van de FOD een overeenkomst afsluit met een externe verwerker, of je voorbereidingen treft om een overheidsopdracht op te starten, moet er voldaan worden aan bepaalde voorwaarden.

Daarvoor neem je contact op met de dienst Overheidsopdrachten (van de stafdienst B&B) en met de DPO.

Geef alle informatie die je kent over de verwerker door, zoals bijvoorbeeld:

* over welke externe verwerker(s) gaat het?
* wanneer start en eindigt de overeenkomst?
* welke (persoons)gegevens worden verwerkt of uitgewisseld?
* wie zijn de contactpersonen bij de externe verwerker?

Starten we in de FOD met een nieuwe opdracht of verwerking?

Dan denken we best vooraf na over de privacy-aspecten en de GDPR-regels die we moeten toepassen. Dit geldt ook voor de wijziging van een bestaande opdracht, wanneer het soort gegevens dat we verwerken, of de manier van gegevens verwerken veranderen.

Projectleiders en betrokken diensten moeten hier dus steeds aan denken, vanaf het vormgeven en organiseren van een opdracht.

Als we persoonsgegevens verwerken moeten we dedocumenteren, zoals eerder reeds vermeld werd.

Wat moeten we nagaan?

* Gaan we persoonsgegevens verwerken? Zo ja, welke? Of gaan we ze anders verwerken dan voordien?
* Hebben we een juridische basis voor de verwerking? Zo ja,welke? (bijvoorbeeld een wettelijk kader, of de toestemming van de betrokkene)
* Welke privacy-risico’s zien we? Bijvoorbeeld op het vlak van confidentialiteit, integriteit en het beschikbaar blijven van de gegevens
* Welke voorbereidende maatregelen nemen we voor een veilige verwerking?
* Al dan niet door een externe verwerker, zoals bijvoorbeeld de beveiliging van de toegang tot de gegevens?
* Welke voorbereidende maatregelen nemen we om efficiënt en op een transparante manier vragen van burgers te kunnen beantwoorden?

Heb je over alle vragen nagedacht? Contacteer zeker ook onze DPO, die je kan helpen en ondersteunen hierbij!

Heb je erover nagedacht welke vragen je gaat stellen? Contacteer zeker ook onze DPO, die je kan helpen en ondersteunen hierbij!

Blijf steeds alert ...

Informatieveiligheid en privacy-bewaking is een zaak van iedereen, blijf daarom steeds alert en respecteer ten allen tijde volgende afspraken!

**Voorkom ten eerste inbraak:** zorg voor een sterk paswoord, en deel het NIET! Zet steeds je schermbeveiliging aan, zodat niemand in je afwezigheid je pc kan gebruiken. Rapporteer verlies of diefstal altijd meteen. Let op met het openen van e-mails, laat je niet vangen door phishing-mails. Let op met surfen op het internet, en bescherm ook je smartphone.

**Voorkom ten tweede informatielekken:** druk steeds belangrijke documenten af via beveiligd afdrukken, laat geen documenten slingeren! Ook niet op bureaus, pas steeds het clean desk principe toe. Vermijd het doormailen van bijlagen, sla documenten op op onze beveiligde locaties en stuur hyperlinks aan collega’s. Vermijd het doorgeven van USB-sticks, CD’s of DVD’s met belangrijke informatie. Let ook op met het doormailen van persoonsgegevens, je e-mail kan verkeerd terecht komen.

**En, voorkom tenslotte schending van de privacy:** bewaar informatie die gelinkt is aan de Kruispuntbank van de Sociale Zekerheid (KSZ) of applicatieve databanken nooit in de Cloud, let op je privacy-settings, bijvoorbeeld op sociale media en surf incognito