
GDPR

Qu’est ce que le RGPD?

- **Règlement Général pour la Protection des données (GeneraI Data Protection Regulation - GDPR)**
- **Nouvelle réglementation avec des règles plus strictes** qui vise à mieux gérer, traiter et protéger les données personnelles des citoyens européens
- Le RGPD est une révision de la législation Européenne de 1995, à présent sous la forme d’ une règlementation au lieu d’une directive.

QUI est concerné par le RGPD?

Le RGPD est d'application pour toutes les **entreprises, organisations, autorités ou personnes** qui rassemblent, traitent et gèrent des données personnelles, quelle que soit leur taille (exception faite des activités strictement personnelles ou domestiques)

Le RGPD est d'application pour toutes les opérations de traitement en Europe (Espace Economique Européen) ou pour le traitement des données des citoyens EU

RGPD – Liste de contrôle

- 1-Inventaire des données personnelles et régistration des opérations de traitement.
- 2-Déclaration de confidentialité
- 3-Sécurité adéquate des données
- 4-Contrat de sous-traitance
- 5-Procédure pour les fuites de données
- 6-Préservation des droits des personnes concernées
- 7-Sensibilisation des collaborateurs
- 8-Etre RGPD conforme en tant qu'Entreprise

DONNEES PERSONNELLES

Données personnelles

- Données concernant une personne physique (ne concerne ni une organisation, ni une association, ni une entreprise).

Par ex: les personnes de contact d'un client, d'un client potentiel, les personnes de contact d'un fournisseur, de collaborateurs etc…

- Identifier (nom, adresse,…) ou identifiable (dérivé des données)
- Toutes les informations (digitales, papiers, images ou sonores…)
- En rapport avec une personne

Egalement indirectement, via un lien (par ex. des données de localisation)

Données personnelles particulières

- **Catégories particulières**
  - Race ou ethnicité
  - Orientation sexuelle
  - Santé et vie sexuelle
  - Opinion politique ou adhérence à un syndicat
  - Conviction religieuse ou philosophique
  - Données d'identification (ADN, données biométriques)
  - Antécédents criminels
- **Autres données sensibles**
  - Données concernant les enfants
  - Données confidentielles (informations financières, données de la carte bancaire…)

1-REGISTRE DES OPERATIONS DE TRAITEMENT

Etablissement du Registre

- Inventaire des données personnelles
- Enregistrer par but
  - Description du but (justification du fait que les données personnelles doivent être traitées)
  - Les catégories concernées (client, prospection, collaborateur) ainsi que la quantité approximative
  - Quel genre de données? Mentionnez certainement si des données particulières ou sensibles sont présentes.
  - Quelles opérations de traitement ont eu lieu ?
  - Durée de stockage des données?
  - Qui a accès aux données: collaborateurs, sous-traitants, destinataires?
  - Des mesures de protection spécifiques?
  - Hors EER?
- Conseil: en dehors des renseignements légaux obligatoires, ajoutez le fondement juridique ainsi que l'analyse de risque

  Base juridique (voir plus loin)

  Estimation des risques

Registre – Exemple vous recevrez ce registre en FR plus tard

AVG Verwerkingenregister

Groepen van personen	Persoonsgegevens	Grondslag verwerking	Verwerking	Bewaartermijn	Verwerking door wie	Verwerking door derden	Verwerking buiten de EU	ICT-systemen	Technische en organisatorische beveiligingsmaatregelen	Toelichting
Deze velden worden gebruikt voor het opstellen van de privacy policy					***Deze velden zijn voor intern gebruik om o.a. de autorisatie matrix op te stellen***					
Benoem groepen van personen van wie je persoonsgegevens ontvangt.	*Benoem de persoonsgegevens die je ontvangt. Maak de **bijzondere persoonsgegevens** vetgedrukt.*	*Wat is de basis die van toepassing is: Uitvoering van een overeenkomst of toestemming of wettelijke verplichtingetc.*	*Beschrijf in globale termen wat je met de persoonsgegevens doet.*	*Beschrijf hoe lang je de gegevens bewaart nadat de overeenkomst is beeindigd.*	*Beschrijf met globale rollen wie de gegevens verwerkt.*	*Als een deel van de verwerkingen door derden wordt uitgevoerd, beschrijf dan hier welke partijen dat zijn.*	*Geef aan of gegevens worden doorgegeven landen buiten de EU.*	*In welke ICT-systemen worden de persoonsgegevens opgeslagen of verwerkt.*	*Beschrijf hoe de persoongegevens beveiligd zijn, zowel technisch asl organisatorisch*	
Hieronder zijn al een aantaal voorbeelden ingevuld. Wat niet van toepassing is kun je verwijderen of aanpassen. Ook kun je nieuwe regels toevoegen. Probeer de beschrijving globaal te houden.										
Als je meer dan 10 doelbindingen nodig hebt, kijk dan nog even goed of je deze niet kunt samenvoegen.										
Klant of leverancier.	Naam, Adres, Woonplaats, Telefoon, E-mailadres	Opdracht of contract.	Administratie, bevestiging, uitlevering.	Gedurende de looptijd van de overeenkomst.	Afdeling administratie, afdeling sales en afdeling inkoop, financiële administratie.	n.v.t.	n.v.t.	Relatiebeheersysteem, Boekhoudsysteem.	Usernaam en wachtwoord op alle sytemen, autorisatie procedure en back-up procedure.	
Verenigingsleden	Naam, Adres, Woonplaats, Telefoon, E-mailadres	Lidmaatschapsovereenkomst	Ledenadministratie, contributieheffing, informatieverstrekking en uitnodigingen voor bijeenkomsten.	Gedurende de periode van het lidmaatschap en daarna alleen in de financiele administratie voor maximaal 7 jaar.	Afdeling ledenadministratie, afdeling communicatie en financiële administratie.	n.v.t.	n.v.t.	Relatiebeheersysteem, Boekhoudsysteem.	Usernaam en wachtwoord op alle sytemen, autorisatie procedure en back-up procedure.	
Nieuwsbrief abonnees.	Naam, E-mailadres	Aanmelding voor nieuwsbrief (formulier op de website met akkoordvinkje voor privacy policy).	Informatie verstrekking in de vorm van nieuwsbrieven.	Gedurende de periode dat men aangemeld is.	Afdeling communicatie.	n.v.t.	n.v.t.	Relatiebeheersysteem, Mailchimp.	Usernaam en wachtwoord op alle sytemen, autorisatie procedure en back-up procedure.	
Prospect, stakeholder-/lobbycontacten en geïnteresseerde.	Naam, Adres, Woonplaats, Telefoon, E-mailadres	Mondelinge toestemming, afgifte visitekaartje en/of via LinkedIn.	Informatieverstrekking in de vorm van nieuwsbrieven of gerichte contacten.	Gedurende de periode dat men contact heeft.	Afdeling communicatie, directie, vakkennisafdelingen en/of relatie beheerder.	n.v.t.	n.v.t.	Relatiebeheersysteem, Mailchimp.	Usernaam en wachtwoord op alle sytemen, autorisatie procedure en back-up procedure.	
Abonnee houders	Naam, Adres, Woonplaats, Telefoon, E-mailadres	Abonnement overeenkomst	Administratie en afdeling communicatie	Gedurende de contract periode en daarna alleen in de financiële administratie voor maximaal 7 jaar.	Administratie en financiële afdeling	Extern verzendhuis voor verzending	n.v.t.	Relatiebeheersysteem	Usernaam en wachtwoord op alle sytemen, autorisatie procedure en back-up procedure.	
Medewerker.	Naam, Adres, Woonplaats, Telefoon, E-mailadres, Geboortedatum, **kopie ID** en Bankgegevens.	Arbeidsovereenkomst.	Salariëring.	Gedurende de periode dat men een contract heeft en daarna alleen in de financiele administratie voor maximaal 7 jaar.	HRM-afdeling, financiële administratie.	n.v.t.	n.v.t.	Relatiebeheersysteem, Boekhoudsysteem.	Usernaam en wachtwoord op alle sytemen, autorisatie procedure en back-up procedure.	

Base juridique

- Obligation juridique
- Effectuer un accord
- Intérêt général
- Importance vitale
- Consentement
- Intérêt légitime

Consentement ou Intérêt légitime

- Consentement
  - Plus ouvert et transparent
  - Beaucoup de conditions
  - Sans consentement actif pas de traitement
  - Peut toujours être retiré
- Intérêt légitime
  - Evaluer les risques- argumentation
  - Contestable
  - Législation plus sévère pour les communications électroniques (ePrivacy)

Questions consentement– quand?

- E-mailings:
  - Clients existants: opt-out
  - Prospection: opt-in
- Mailings via la poste:
  - Toujours la règle opt-out
  - Attention: respect de la liste Robinson

Question consentement– comment?

- Informé et spécifique
  - Information au préalable au sujet du but et de la nature du traitement, durée, destinataires
  - Consentement bien séparé pour chaque traitements différents
  - Information au sujet du risque et des mesures de sécurité – certainement lors d'un transfert hors EER
- Actif
  - Cochez manuellement le consentement (pas coché en avance)
- Libre
  - Le consentement ne peut pas déterminer si un service est accordé ou pas
- Possibilité de retrait
  - Le retrait doit être aussi facile que de donner le consentement

2-DECLARATION DE CONFIDENTIALITE

Déclaration de confidentialité

- Une déclaration de confidentialité va veiller à ce que le client sache où il en est en terme de confidentialité. Un éclaircissement au sujet de ce que vous faites des données personnelles des visiteurs et des clients.
- Une déclaration de confidentialité doit correspondre aux caractéristiques suivantes:
  - brève
  - transparente
  - compréhensible
  - Facile d’accès

Déclaration de confidentialité

- La déclaration de confidentialité de l'organisation doit être accessible pour tous. Le plus simple est de l'ajouter sur le site web de l'organisation et d'ajouter un lien sur chaque page (en dessous)

- Un rapport avec la déclaration de confidentialité doit figurer dans tous les accords (documents dans lesquels des données personnelles sont reprises)

Déclaration de confidentialité - Contenu

- Description exacte et coordonnées du DPO responsable ou de la personne de contact.
- Description des traitements (suffisamment subdivisés)
  - Par but: genre de données, nature du traitement, délai de stockage, destinataires des données.
  - Par but également la base juridique (“par intérêt légitime “ à évaluer avec le droit de confidentialité)
- Description des mesures de sécurité
- Déclaration des droits de la personne concernée
  - L'énumération de ses droits.
  - Procédure pour introduire une demande
  - Déclaration du droit de pouvoir introduire un recours auprès des autorités du traitement des données
- Indiquez si les données peuvent être utilisées hors EER.

Déclaration de confidentialité - Interne

- Les collaborateurs sont également concernés.
- Etablissez une déclaration interne de confidentialité (info similaire)
  - Procédure ou instruction de travail (de préférence à ne pas intégrer dans les accords de travail)
  - N'oubliez pas les données telles que des emails (contenu/ métadonnée) et traçabilité des activités sur Internet, en application ou sur les appareils mobiles.
- Discutez également de leurs droits en tant que personne concernée
  - Procédure interne pour les collaborateurs
  - Procédure pour soumettre une demande
  - Une mention du droit de pouvoir introduire une plainte auprès de l'autorité du traitement des données
- Plus grandes sociétés
  - Discutez-en lors du conseil d'entreprise
  - Faites éventuellement signer avec une mention ' lu et approuvé '

3-SECURITE ADEQUATE DES DONNEES

Des mesures de sécurité appropriées

- **En tant qu'organisation veillez à établir des mesures de sécurité techniques et organisationnelles** afin d'atteindre un niveau de sécurité qui correspond au risque
- Tenez-en bien compte avec l'état actuel de la technique, des coûts d'implémentation, ainsi que la nature, le champ d'application, le contexte, les objectifs du traitement et les risques des droits et libertés des personnes. Ce faisant, vous devez bien penser aux mesures de sécurité adaptées suivantes
  - Toutes les données personnelles ne sont accessibles qu'avec un inlog, qui peut être un mot de passe sur un téléphone ou un nom d'utilisateur et mot de passe sur un ordinateur
  - Utilisez le plus possible des supports de données cryptés si vous devez exporter des données personnelles spécifiques. Dans ce cas, les données personnelles ne sont pas lisibles pour les autres
  - Utilisez des sécurités sur les dossiers réseaux ainsi qu'où c'est nécessaire pour les fichiers réseaux
  - Envisagez de mettre en place plusieurs authentifications (introduction d'un code en plus du nom d'utilisateur et du mot de passe, que vous recevez per exemple par SMS)

Des mesures de sécurité appropriées

- Verrouillez le site web/ le réseau pour les pays où ce n'est pas strictement nécessaire. Conseil : il est possible de fermer le trafic internet de l'organisation pour les pays où les pirates informatiques sont fort actifs.
- Lorsque les données personnelles sont accessibles via un site web déterminé, la connection internet sécurisée doit être reconnaissable via le verrou informatique (en vert en HTTPS)
- Si vous devez sauver des données personnelles spécifiques dans votre CRM, veillez à ce qu'elles ne soient visibles uniquement que par la personne désignée (avec autorisation)
- Veillez à ce qu'une bonne procédure de backup soit mise en place avec, entre-autre, des tests réguliers du rétablissement des données
- Testez et évaluez régulièrement les mesures de sécurité

Evaluation des risques

- Analysez les risques possibles
- Associez des mesures de sécurité à ces risques
- Coûts et efforts proportionnellement à un impact possible
- Evaluez au minimum 1 fois par an
- Apprenez de vos erreurs et incidents

Mesures organisationnelles

- Formation et sensibilisation du personnel
  - Screening – contrat de confidentialité - formation
- Sécurité physique, contrôle d'accès, zonage des bâtiments
- Contrôle des sous-traitants
  - Sélection – accord de sous-traitance - Contrôle
- Procédure change management
- Incident management (voir plus loin)
- Amélioration continue

Mesures Techniques

- Echange de données
    - Cryptage (https, sftp) vs annexe d'email ou plateforme publique
    - Connections VPN / lignes réservées
    - Protection des systèmes et réseaux
    - Firewall / Virus scanning / Content filtering
    - Zones séparées
    - Authentification sécurisée / autorisation matrix sur base des fonctions
- Monitoring et traçabilité
    - Contrôle de la disponibilité et du bon fonctionnement
    - Contrôle lors d'évent sécurisés ou d'activité sur le réseau
    - Traçabilité des déplacements des données ou des activités du système administrateur
- Grande disponibilité, backup et disaster recovery
- Suppression permanente des données

Conseils pour la suppression des données

- Faites un relevé de tous les systèmes qui comprennent des données personnelles
- Faites bien attention au fait que les backup sont également concernés

- Veillez à avoir le moins possible de petites listes séparées. Indiquez sur les listes combien de temps elles restent valables et comment elles peuvent être détruites
- Laissez nettoyer automatiquement les boites mail et effacez régulièrement les anciens contacts
- Convenez d'avoir en permanence des données à jour dans le système CRM qui peuvent être consultées.
- Veillez à avoir une procédure claire du nettoyage du CRM. Si une personne ne peut être effacée, supprimez tous les champs reliés à cette personne et mettez un texte type dans le champs « nom » de façon à ce que sachiez qu'il s'agit d'une personne effacée
- Passez un arrangement avec une tierce personne par le biais des accords de sous- traitance que des fichiers à usage unique seront supprimés ultérieurement (par exemple dans le fichier des adresses donné à un imprimeur pour l' envoi d'un mailing)
- Convenez avec vos collaborateurs et fournisseurs software que les données peuvent être vraiment supprimées

4-ACCORDS DE SOUS-TRAITANCE

Accord de sous-traitance

- En tant qu'organisation, vous ne pouvez transmettre de données personnelles à une autre partie **sans un accord de sous-traitance**. Vous convenez lors d'un accord de sous-traitance de ce que l'autre peut ou ne peut pas faire avec les données.
- Vous pouvez partager les données avec une tierce personne que si c'est nécessaire pour la réalisation des objectifs pour lesquels vous les avez reçues
- **CONSEIL: faites d'abords un schéma de votre système de décor**. Vous aurez ainsi un aperçu de tous les accords de sous-traitance à faire.

Accord de sous-traitance

- Dispositions importantes
  - Qui est responsable et qui est sous-traitant
  - Déclaration de confidentialité
  - Interdiction de traiter les données sans un mandat écrit
  - Sécurisation adéquate à réaliser
  - Interdiction de transmettre les données, sauf si sous-traitance (après approbation)
  - Suppression permanente des données après mandat (démontrable)
  - Obligation d'une mention perte de données ou presque perte de données
  - Interdiction de communiquer en direct avec les autorités ou les personnes concernées (uniquement via le responsable)
  - Droit d'audit

Accord de sous-traitance

- Annexes
  - Description claire de la tâche
    - quelles sont les traitements à faire
    - description du type de données et les catégories des personnes concernées
    - délai de conservation des données
  - Description des mesures de sécurité appliquées
    - L'information sur la politique de sécurité
    - Les certificats éventuels
  - Dispositions pour la disponibilité / Comment supprime-t-on les données
  - Accords pour la déclaration de fuite de données
    - Formulaire de déclaration
    - Les coordonnées du délégué à la protection des données (DPO)

5-PROCEDURE CONCERNANT LES FUITES DE DONNEES

Fuites de données

- **Qu’est-ce qu’une fuite de donnée?**

Une fuite de données est une violation de la sécurité des données personnelles. Une fuite de données est un incident de sécurité durant lequel des données personnelles ont été divulguées. Cela peut partir d’un accès non autorisé jusqu’à la destruction, une modification ou la dissémination de données personnelles. Nous ne parlons d’une fuite de données que lorsque des données personnelles ont été divulguées !

Exemples de fuites de données

- Vous perdez un stick USB-stick sur lequel se trouve des données personnelles.
- Un Pc portable sur lequel se trouvent des données personnelles a été dérobé.
- Un fichier ou système reprenant des données personnelles a été piraté.
- Des papiers comportant des données personnelles ont été volés dans un sac.
- Des données personnelles ont été perdues suite au crash du disque dur ou lors d’un incendie et il n’y a malheureusement pas de back-up.

Fuites de données – incident management

- Limitez l'impact
  - Arrêter le traitement erroné (arrêter la machine ou le serveur, interrompre la connection,…)
  - Arrêter le transfert de données (empêcher la délivrance postale, retirer la page web, fermer l'accès, rappeler l'envoi)
- Analysez l'incident
  - Est-ce que des données personnelles sont concernées? Si oui, sont-elles sensibles ou exceptionnelles ? Combien ?
  - Il y a-t-il eu effectivement une fuite de données? Quelle en est l'ampleur ?
  - Il y a-t-il un impact ? Est-ce que les données sont cryptées ? Ou pseudonymisées ?
- Dégénérer
  - Des données personnelles sont concernées? Il faut toujours faire appel au responsable DPO
  - Etes-vous sous-traitant? Il faut toujours faire appel au responsable
  - Il y a-t-il une déclaration?
- Déterminez-en l'origine et cherchez la solution
- Evaluez et établissez un plan l'amélioration

Fuites de données – Obligation de déclaration

- Un incident mais pas une fuite de données
  - Notez l'incident sur votre liste interne d'incidents
  - Mais faites un rapport avec la cause, la solution, le plan d'amélioration (et le suivi)
  - Le signalez éventuellement au responsable
- Une fuite de données mais pas d'impact
  - Idem voir premier point
  - Faites toujours appel au responsable DPO
  - Etes-vous sous-traitant? Avertissez (endéans les 24h) le responsable
  - Vous êtes le responsable? Une déclaration n'est pas nécessaire (mentionnez l'argumentation dans votre rapport)
- Une fuite de données avec un impact (grave)
  - Etes-vous sous-traitant? Assistez le responsable – ne communiquez jamais vous-même
  - Vous êtes le responsable? Le responsable DPO fait la déclaration endéans les 72h
  - Est-ce grave ou non? Il y a une déclaration ou pas? Le responsable DPO vous conseille – notez l'argumentation à suivre
- Une fuite de données et un haut risque de dégâts
  - Idem voir point 3
  - Vous êtes le responsable? Contactez si possible immédiatement les personnes concernées

Fuites de données – procédure

- Etablissez une procédure pour le traitement des fuites de données
  - Déterminez les rôles et responsabilités
  - Fixer le critère pour une escalade
- Sous-traitant? Notez les coordonnées du responsable DPO dans votre registre
  - Par nom et coordonnées du responsable DPO
  - Par type de compétence des données
  - Notez si le responsable exige une mention lors d'une presque- fuite de données
- Responsable? Que devez-vous mentionner?
  - La nature de l' incident
  - Le genre de données et le genre des personnes concernées (ainsi que la quantité impactée
  - L'impact réel et possible
  - Les mesures prises afin de limiter l'impact
  - Les coordonnées de votre propre responsable DPO
- Formez le personnel
  - Comment reconnaitre un incident?
  - Qui devez-vous prévenir?

6-PROTECTION DES DROITS DE LA PERSONNE CONCERNEE

Droits de la personne concernée

- Transparence
  - Information au sujet des opérations de traitement
- Droits relatifs aux données propres
  - Le droit de regard
  - Le droit de rectification
  - Le droit à l'oubli
  - Le droit à la limitation du traitement
  - Le droit à l'obligation de notification
  - Le droit à la portabilité des données
  - Le droit de recours

Droits de la personne concernée - Procédure

- Comment se déroule une demande?
  - La personne concernée doit trouver la méthode de travail appropriée facile
  - Les collaborateurs internes doivent savoir canaliser les questions
  - Une fluidité harmonieuse doit à veiller à un traitement à terme fixe (30 jours)
- Comment faut-il traiter une demande?
  - Définissez quelle info se trouve à quel endroit
  - Fixer un critère pour traitement des demande ou non
  - Etablissez une justification standard pour les rejets
- Comment assurer le suivi?
  - Conservez une liste des actions des demandes, réponses et motivations (ainsi que le statut)
  - Evaluez le processus et établissez un plan d'amélioration

7-SENSIBILISATION DES COLLABORATEURS

Informez les collaborateurs de leurs obligations

Qu'est-ce que l'on attend de vous en tant que collaborateur?

- La signature de la clause de confidentialité (celle-ci peut faire partie de l'accord de travail)
- Tenez-vous aux règles de votre politique de confidentialité
- N'utilisez les données personnelles uniquement que pour le but pour lequel elles ont été données
- Dispersez les documents comprenant des données personnelles si ceux-ci ne doivent plus être conservés
- Ne donnez jamais des données personnelles à de tierces personnes sans accord de sous-traitance
- Ne sauvegardez jamais des données personnelles sur un serveur ou sur des services online hors EU
- Veillez à ce que vos ordinateurs et anti-virus soient et restent à jour

Donnez aux collaborateurs des lignes conductrices pratiques

Les points repris ci-dessous sont valables pour chaque personne qui fait partie de votre organisation.

Conseil : faites une fiche (plastifiée) reprenant ces informations pratiques et affichez en une à chaque poste de travail

- Verrouillez à chaque fois votre écran lorsque vous quittez votre poste de travail
- Ne laisser jamais des documents comprenant des données personnelles sur votre bureau ou sur l'imprimante
- Ne choisissez jamais une sauvegarde automatique de vos identifiants sur votre ordinateur
- Réalisez bien que les réseaux publics ne sont pas sûrs
- Faites attention à ce que vous partagez via le social média
- Protégez votre webcam afin d'éviter tout piratage
- N'utilisez jamais le login de vos collègues et ne leur transmettez jamais le vôtre
- Veillez à ce que votre téléphone portable soit protégé par un mot de passe (code login)

Procédure – Formation du personnel

- Organisez une formation d'introduction pour les nouveaux collaborateurs
- Répétez au minimum une fois par an cette formation
- Utilisez des affiches ou des tableaux informatifs afin de donner des conseils
- Rédigez une brochure
- Organisez un séance d'exercice ou un quiz
- N'oubliez pas les intérimaires, les collaborateurs temporaires et les consultants

8-ETRE CONFORME

Qu’est ce qui fait de vous un RGPD-conforme?

- Nous disposons d’un **registre des données**
- Notre **politique de confidentialité** est adaptée
- Les **mesures techniques et organisationnelles** nécessaires sont installées pour la protection des données personnelles
- Nous vous avons envoyé un **accord de sous-traitance** dans lequel il est bien clairement stipulé à quelles fins vous pouvez utiliser les données personnelles
- Le **responsable des données à caractère personnel** dans notre organisation est : XXX
- Nous avons une procédure dans laquelle il est clairement stipulé ce qui doit se faire en cas de **fuite de données**
- Nous avons une règlementation qui veille à ce que nous puissions garantir **les droits des personnes concernées**
- Notre personnel est au courant de **l’importance du RGPD,** des procédures internes, des obligations légales et particulièrement du fait que les données à caractère personnel sont confidentielles et protégées

Pouvez-vous également le démontrer?

- Avez-vous assez de connaissance en la matière?
- Est-ce que le responsable DPO a reçu une attestation lors de sa formation ? (pas nécessaire)
  - Avez-vous conservé les listes (et évaluations) des participants lors de la formation interne ?
- Sur quel but et sur quel fondement juridique se base chaque traitement des données?
- Avez-vous pesé les risques du traitement et y avez-vous aligné votre sécurité ?
  - Disposez-vous d'une description de votre analyse de risque ?
  - Quand est-ce que celle-ci a été actualisée pour la dernière fois ? Quel plan d'action a été mis en place à ce moment-là ?
- Pouvez-vous démontrer que vous contrôlez votre sécurité et que vos mesures sont suffisantes?
- Avez-vous un registre interne des incidents (et des fuites des données), avec évaluation ?
- Avez-vous en tant qu'autorité responsable des sous-traitants, en votre possession:
  - Un rapport screening/ un accord de sous-traitance / une évaluation du fournisseur
- Précisez-vous de quelle manière vous avez traité chaque demande d'une personne concernée ?

Pour conclure….

- **Le RGPD est un texte législatif aussi dense que compliqué.**
- Ce plan par étape **est un explicatif ainsi qu'une interprétation fortement comprimés.** Nous ne pouvons garantir que toutes les explications sont toujours tout-à fait exactes, complètes et actuelles.
- Les informations données sont destinées à être utilisées en tant qu'**information générale** et sont fournies à titre informatif.
- Ces informations peuvent nous aider à **renforcer et améliorer l' image concernant la réglementation des garanties de confidentialité** ainsi que la mise en place et en œuvre de votre politique de confidentialité.
- Cette présentation ne peut pas être vue en tant que conseil juridique concret.
- Le texte législatif RGPD reste bien évidemment votre guide de référence officiel

KEEP CALM AND COMPLY WITH GDPR

FEBELGRA - AGALLIS

BNP PARIBAS FORTIS

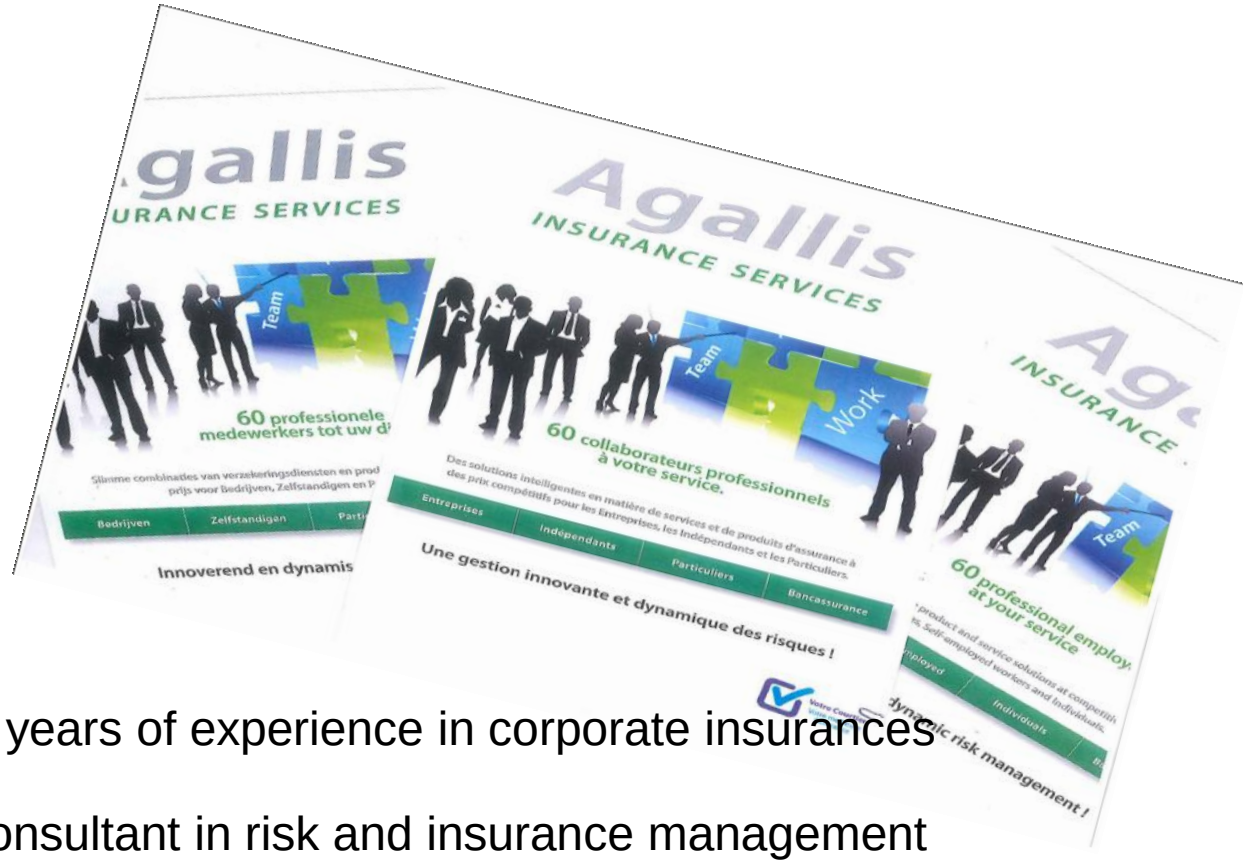
Agallis INSURANCE SERVICES

PRESENTATIE GDPR – CYBERVERZEKERING

2 MEI 2018 – BIZNIS HOTEL LOKEREN

BNP PARIBAS FORTIS

AGALLIS nv



- More than 80 years of experience in corporate insurances
- Broker and consultant in risk and insurance management
- Access to all insurance markets
- Continuously trained professional (technical and legal staff
- Complaint management

BNP PARIBAS FORTIS

ICT CARE – FULL PROTECTION

Feiten

31 % van de AANVALLEN	MGO < 250 FTE's
60 % van de KMO's	Stoppen na cyberattack
85 % verlies/diefstal data	KMO = slachtoffer
Dagelijks	4.000 Ransomeware attacks

BNP PARIBAS FORTIS

INCIDENT RESPONSE PLAN

Voorbereidingsfase

- Identificatie van wat er moet worden beveiligd (netwerk, producten, ...)
- Identificatie en toewijzing van verantwoordelijkheden
- Interne bekwaamheden bepalen of cont(r)acten met externe experts

Incidentdetectiefase

- technologie om een cyberveiligheidsincident te detecteren

BNP PARIBAS FORTIS

INCIDENT RESPONSE PLAN

Incidentinperking

- De systemen onmiddellijk loskoppelen om zo snel mogelijk te herstellen ?
- Of de tijd nemen om de bewijzen te verzamelen tegen de cybercrimineel ?

Risicobeperking en herstel

- Een communicatiestrategie voor belanghebbenden voor autoriteiten zoals ordehandhavers en de Privacy commissie

een CYBERVERZEKERING afsluiten.

De kosten van cyberveiligheidsincidenten lopen vaak op tot honderdduizenden.
Een betrouwbare cyberverzekering dekt deze kosten.

BNP PARIBAS FORTIS

ICT CARE – FULL PROTECTION

Eigen schade

Bedrijfsstilstand	Garantie bedrijfscontinuïteit
Hardware – Data / Software	Wedersamenstellingskosten…
Herstelkosten	Extra personeel, virusvrij maken, …
Reputatieschade	Public relations acties …
Afpersing	Afpersingscoördinator, advocaat

BNP PARIBAS FORTIS

ICT CARE – FULL PROTECTION

Aansprakelijkheid

Cyberdiefstal

- Beweerde laster, eerroof, schending auteursrecht

Multimedia aansprakelijkheid

- Wedersamenstellingskosten…

Aansprakelijkheid tov derden

- Verdedigingskosten na schade-eis

Privacywetgeving / GDPR

- Meldingsplicht ivm verzamelen persoons- en bedrijfsgegevens
- Kennisgevingskosten

BNP PARIBAS FORTIS

SUMMARY GDPR + ICT CARE

PREVENTIE

=> Incident Response Plan

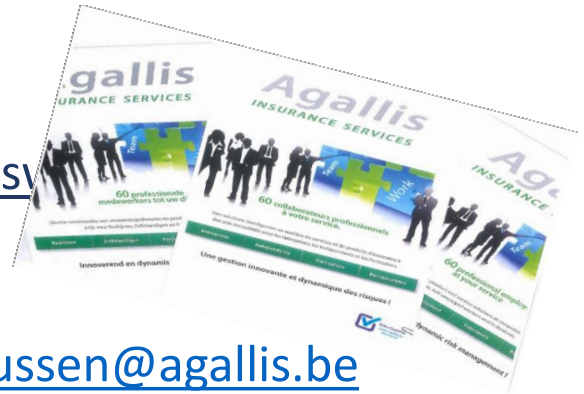
VERZEKERING

- 48 HR FIRST RESPONSE
- EIGEN SCHADE
- AANSPRAKELIJKHEID
- QUOTE PAD CYBEREDGE

BNP PARIBAS FORTIS

UW SPO's - AGALLIS

Francis Rondas – Key Account Manager
francis.rondas@agallis.be
T. +32 2 775 34 08
M. +32 477 38 88 29



Charlien Swinnen – Insurance Advisor charlien.sw
T. +32 2 775 34 26

Raf Meeussen – Senior Manager Sales raf.meeussen@agallis.be
T. +32 2 775 33 18
M. +32 468 35 61 15

BNP PARIBAS FORTIS

QUESTIONS ?

Gegevensbescherming

Voorkom datalekken – confidentiële vernietiging

FEBELGRA, GDPR Sessie
Lokeren, 02/05/18

OUD PAPIER JOZEF MICHEL

- Recuperant oud papier in héél België sinds >65 jaar
- Gespecialiseerd in grafisch papier
- Servicepakket op maat van elke klant
- Investeren in installaties met doel uw efficiëntie te verhogen
- Hoge & correct betaalde opbrengsten voor onze klanten

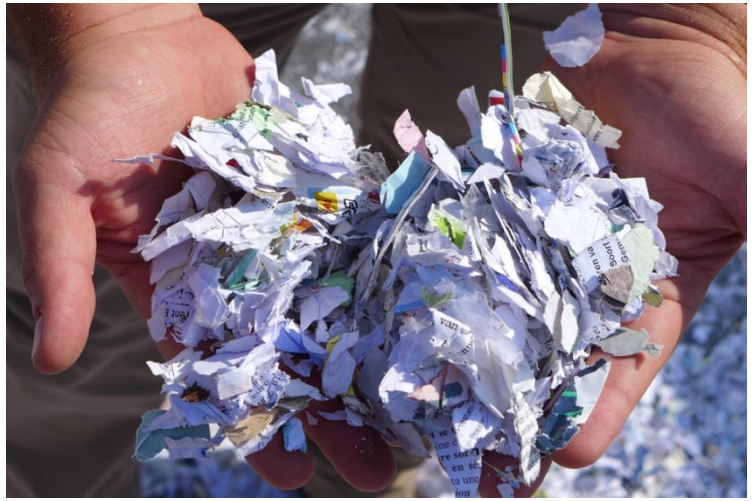
DATAVERNIETIGING MICHEL

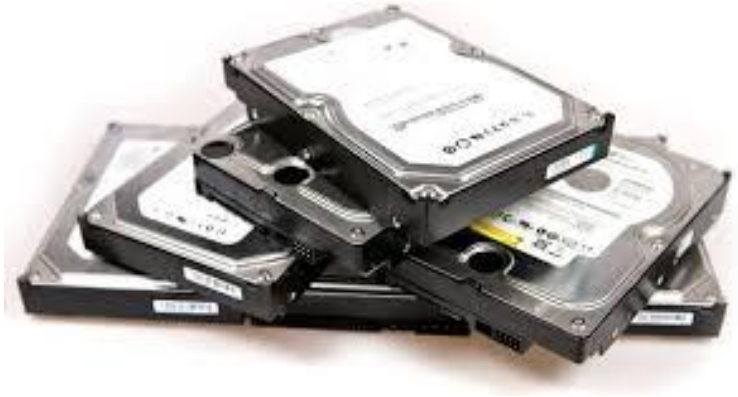
- Eerste data- en archiefvernietiger in België (sinds 1986)
- Vernietiging mét attest van
  - vertrouwelijke documenten & datadragers
- Beveiligd transport en gescreend personeel
- Gewaarborgde veiligheidsprocedures
- High Security Division = uniek in België

DIN66399 Veiligheidsniveaus

Veiligheid	Type data	Type document	Verwerking
Niveau 1	Algemene info	Catalogus/Brochures	Normaal beveiligd
Niveau 2	Interne documenten	Algemene bedrijfsdocumenten	Normaal beveiligd
Niveau 3	Gevoelig & persoonlijk	Verkoop / klant documentatie **PERSOONSGEGEVENS !**	Normaal beveiligd
Niveau 4	Gevoelig & persoonlijk	Loonfiches, medisch/taks docs **PERSOONSGEGEVENS!**	Streng beveiligd
Niveau 5	Confidentieel	Patenten /overheidsgebouwen	Streng beveiligd
Niveau 6	Confidentieel & geheim	R&D documenten	Zeer strenge veiligheidsmaatregelen
Niveau 7	Strikt geheim & top secret	Geheime Diensten	Strengste veiligheidsmaatregelen

DIN66399 Veiligheidsniveaus





	PAPIER / ARCHIEF
P1	Snipper max 12mm lengte
P2	Snipper max 6 mm lengte
P3	Max 320 mm2
P4	Max 160 mm2
P5	Max 30 mm2
P6	Max 10 mm2
P7	Max 5mm2

	HARD DISKS
H1	Mech./electr. Buiten werking
H2	Beschadigd
H3	Vervormd
H4	Shredder <2000mm2
H5	Shredder <320mm2
H6	Shredder <10mm2
H7	Shredder <5mm2

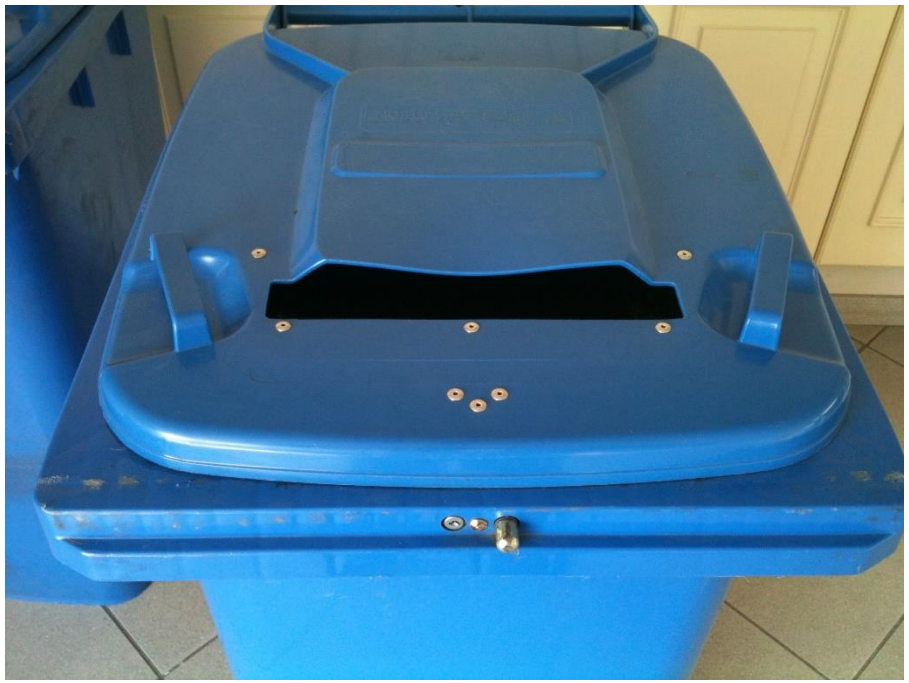
DATAVERNIETIGING MICHEL

GROUP JOOS Unlimited Digital Solutions & Print

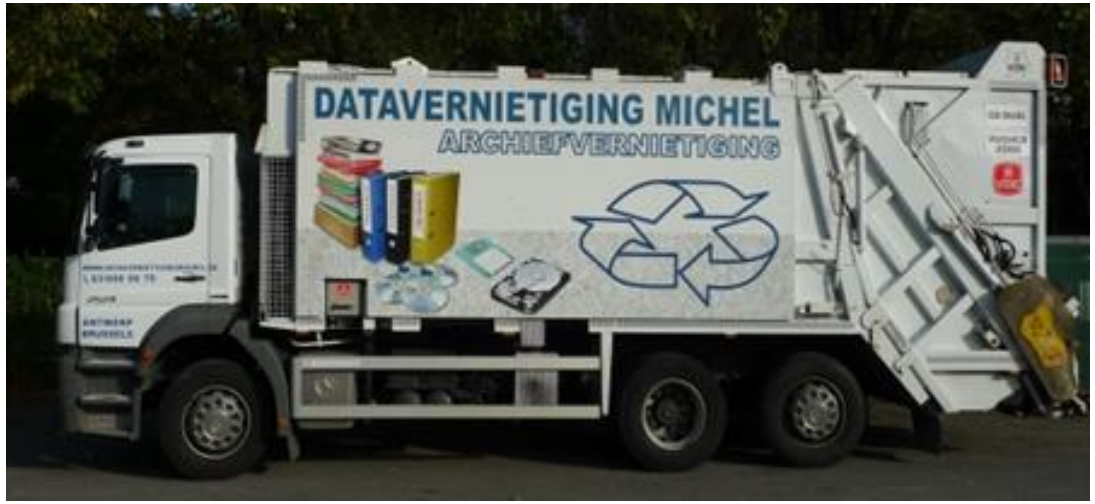
febelgra

Beveiligde inzameling

INTERN



TRANSPORT NAAR DEPOT



DATAVERNIETIGING MICHEL

Beveiligde verwerkingsdepots

DATAVERNIETIGING MICHEL

www.datavernietigingmichel.be

TEL: 03 / 666 96 79