WAT is de GDPR?

- = **General Data Protection Regulation (GDPR)**
- Bepaalt **nieuwe, striktere regels** om de persoonlijke gegevens van Europese burgers beter te beheren, verwerken en beveiligen.
- De GDPR is een herziening van de Europese wetgeving uit 1995, nu een verordening i.p.v. een richtlijn.
- De nieuwe wetgeving wordt ook de ‘Algemene Verordening Gegevensbescherming’ of AVG genoemd.

VOOR WIE is de GDPR?

De GDPR geldt **voor alle bedrijven, organisaties, overheden of personen** die persoonsgegevens verzamelen, beheren en verwerken, onafhankelijk van hun grootte

(met uitzondering van huis-, tuin- en keukengebruik)

De GDPR geldt voor alle verwerkingen in Europa (Europese Economische Ruimte) of van gegevens van EU-burgers

GDPR - checklist

1-Inventaris van persoonsgegevens en register van verwerkingen

2-Privacy verklaring

3-Adequate beveiliging van de gegevens

4-Verwerkersovereenkomsten

5-Procedure rond datalekken

6-Vrijwaren van de rechten van de betrokkene

7-Bewustmaking van de medewerkers

8-GDPR-Compliant zijn als bedrijf

PERSOONSGEGEVENS

Persoonsgegevens

- Gegevens over een natuurlijke persoon (dus niet over een organisatie, vereniging of bedrijf).

  Vb: de contactpersonen van een klant, lead of prospect (potentiële klant), contactpersonen van een leverancier, medewerkers enz.
- Geïdentificeerd (naam, adres…) of identificeerbaar (af te leiden uit data)
- Alle informatie (digitaal, op papier, beeld of klank…)
- In verband met een persoon

  Ook indirect, via koppeling (bijv. locatiegegevens)

Bijzondere persoonsgegevens

- Bijzondere categorieën
  - Ras of etniciteit
  - Seksuele geaardheid
  - Gezondheid en seksueel leven
  - Politieke voorkeur of lidmaatschap van een vakbond
  - Religieuze of filosofische overtuiging
  - Identificatiegegevens (DNA, biometrische gegevens)
  - Crimineel verleden
- Andere gevoelige data
  - Gegevens over kinderen
  - Schadegevoelige gegevens (financiële info, bankkaartgegevens…)

1-REGISTER VAN VERWERKINGEN

Register opstellen

- Inventaris van persoonsgegevens
- Per doel vastleggen
  - Omschrijving van het doel (verantwoording waarom persoonsgegevens moeten verwerkt worden)
  - Categorieën betrokkenen (klanten, prospecten, medewerkers) en geschatte aantallen
  - Welk type data? Vermeld zeker of er gevoelige of bijzondere persoonsgegevens bij zijn
  - Welke verwerkingen gebeuren er?
  - Bewaartijd van data
  - Wie heeft toegang tot de gegevens: medewerkers, onderaannemers, bestemmelingen
  - Specifieke beschermingsmaatregelen
  - Buiten EER?
- Advies: buiten wettelijk verplichte inlichtingen ook grondslag en risicoanalyse toevoegen
  - Wettelijke grondslag (zie verder)
  - Inschaling van risico’s

Register - voorbeeld

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.	

Wettelijke grondslag

- Wettelijke verplichting
- Uitvoeren overeenkomst
- Algemeen belang
- Levensbelang
- Toestemming
- Gewettigd belang

Toestemming of gewettigd belang

- Toestemming
  - Meest open en transparant
  - Veel voorwaarden
  - Zonder actieve toestemming geen verwerking
  - Kan altijd ingetrokken worden
- Gewettigd belang
  - Afwegen tegen risico’s - argumenteren
  - Aanvechtbaar
  - Voor elektronische communicatie strengere wetgeving (ePrivacy)

Toestemming vragen – wanneer?

- E-mailings:
  - Bestaande klanten: opt-out
  - Prospecten: opt-in
- Mailings via de post:
  - Altijd opt-out regel
  - Opgepast: respecteren van de Robinsonlijst

Toestemming vragen – hoe?

- Geïnformeerd en specifiek
  - Vooraf info over doel en aard van verwerking, duur, bestemmelingen
  - Aparte toestemming voor verschillende verwerkingen
  - Info over risico's en beschermingsmaatregelen – zeker bij transfer buiten EER
- Actief
  - Niet stilzwijgend, maar via bewuste handeling
- Vrij
  - Toestemming mag niet bepalen of een dienst al dan niet verleend wordt
- Steeds in te trekken
  - Intrekken moet even gemakkelijk zijn als toestemming geven

2-PRIVACY VERKLARING

Privacy Verklaring

- Een privacyverklaring dient ervoor te zorgen dat een klant weet waar hij aan toe is op het gebied van zijn privacy. Een toelichting over wat je met persoonsgegevens van bezoekers en klanten doet.
- Een privacy verklaring moet voldoen aan de volgende kenmerken:
  - beknopt
  - transparant
  - begrijpelijk
  - gemakkelijk toegankelijk

Privacy Verklaring

- De privacy verklaring van de organisatie moet voor iedereen vindbaar zijn. Het eenvoudigste is om deze op de website van de organisatie te zetten en op elke pagina (onderaan) een link hier naartoe te leggen.
- In alle overeenkomsten (documenten waarin persoonsgegevens gevraagd worden) moet een verwijzing staan naar de privacy verklaring.

Privacy Verklaring - Inhoud

- Exacte omschrijving van de verantwoordelijke en coördinaten van de DPO of contactpersoon
- Beschrijvingen van de verwerkingen (voldoende opgesplitst)
  - Per doel: type data, aard van de verwerking, bewaartermijn, bestemmelingen van de data
  - Per doel ook de rechtsgrond (en bij ‘gewettigd belang’ ook de weging ten opzichte van het recht op privacy)
- Beschrijving van de beveiligingsmaatregelen
- Vermelding van de rechten van de betrokkene
  - Opsomming van zijn rechten
  - Procedure om een verzoek in te dienen
  - Vermelding van recht om klacht in te dienen bij de gegevensverwerkingsautoriteit
- Aanduiding of data buiten EER terecht kunnen komen

Privacy Verklaring - Intern

- Medewerkers zijn ook betrokkenen
- Stel een interne privacy verklaring op (zelfde info)
  - Procedure of werkinstructie (beter niet verwerkt in arbeidsovereenkomst)
  - Vergeet niet data als emails (inhoud / metadata) en loggings van activiteiten op het internet, in toepassingen of op mobiele toestellen
- Bespreek ook hun rechten als betrokkene
  - Interne procedure voor medewerkers
  - Procedure om een verzoek in te dienen
  - Vermelding van recht om klacht in te dienen bij de gegevensverwerkingsautoriteit
- Grotere firma's
  - Bespreek dit in de ondernemingsraad
  - Laat eventueel aftekenen 'voor kennisname'

3-ADEQUATE BEVEILIGING VAN DE GEGEVENS

Passende beveiligingsmaatregelen

- **Als organisatie zorg je voor technische en organisatorische beveiligingsmaatregelen** om een beveiligingsniveau te bereiken dat past bij het risico.
- Hierbij houd je rekening met de laatste stand van de techniek, de kosten van implementatie, evenals de aard, de reikwijdte, de context, de doeleinden van de verwerking en de risico's voor de rechten en vrijheden van personen. Daarbij kun je denken aan de volgende passende maatregelen:
  - Alle persoonsgegevens zijn alleen te bereiken via een inlog, dit kan een wachtwoord zijn op een telefoon of een gebruikersnaam en wachtwoord op een computer.
  - Gebruik zoveel mogelijk versleutelde gegevensdragers als je bijzondere persoonsgegevens moet vervoeren. Hiermee zorg je ervoor dat de persoonsgegevens voor anderen niet leesbaar zijn.
  - Gebruik beveiliging op netwerkmappen en waar nodig ook op bestanden op het netwerk.
  - Overweeg om meervoudige authenticatie in te voeren (naast een gebruikersnaam en een wachtwoord moet dan ook een code ingevoerd worden, die je bijvoorbeeld via SMS ontvangt).

Passende beveiligingsmaatregelen

- Sluit de website/het netwerk af voor landen waarvoor dit niet strikt noodzakelijk is. Toelichting: het is mogelijk om internetverkeer naar de organisatie af te sluiten voor landen waar vandaan veel hackers actief zijn. Werk hierbij van binnen naar buiten, dus alleen openstellen voor landen waarvoor dat stikt noodzakelijk is.
- Als persoonsgegevens via een besloten website te benaderen zijn, moet die beveiligde internetverbinding te herkennen zijn aan het groene slotje (HTTPS).
- Als je bijzondere persoonsgegevens in je CRM opgeslagen hebt, zorg er dan voor dat deze alleen door de juiste personen (met autorisatie) te zien zijn.
- Zorg voor een goede back-up procedure met onder andere een regelmatige test van het herstellen van de gegevens.
- Test en evalueer regelmatig de maatregelen en de beveiliging.

Risicobeoordeling

- Analyseer de mogelijke risico’s
- Koppel beveiligingsmaatregelen aan deze risico’s
- Kosten en inspanningen in verhouding tot de mogelijke impact
- Evalueer minstens 1 maal per jaar
- Leer uit fouten en incidenten

Organisatorische maatregelen

- Opleiding en awareness van personeel

  Screening – Vertrouwelijkheidsovereenkomst - Opleiding
- Fysieke beveiliging, toegangscontrole, zonering van gebouwen
- Controle op onderaannemers

  Selectie – Verwerkersovereenkomst - Controle
- Change management procedure
- Incident management (zie verder)
- Continue verbetering

Technische maatregelen

- Datauitwisseling
  - Encryptie (https, sftp) vs Email-attachment of publiek platform
  - VPN-verbindingen / dedicated lijnen
- Beveiliging van systemen en netwerk
  - Firewall / Virusscanning / Content filtering
  - Gescheiden zones
  - Veilige authenticatie / autorisatiematrix op basis van functies
- Monitoring en logging
  - Controle op beschikbaarheid en goede werking
  - Controle op security events of activiteit op netwerk
  - Logging van databewegingen of activiteiten van system administrators
- High availability, backup en disaster recovery
- Permanent verwijderen van data

Tips voor het Verwijderen van gegevens

- Maak een overzicht van alle systemen waarin persoonsgegevens gebruikt worden.
- Let er op dat ook de back-ups in dit verhaal betrokken worden
  - Zorg voor zo min mogelijk losse lijstjes. Geef op lijstjes aan hoe lang deze ‘houdbaar’ zijn en hoe deze vernietigd moeten worden;
  - Laat mailboxen automatisch opschonen en laat ook regelmatig oude contacten verwijderen;
  - Spreek af dat je altijd zorgt voor actuele gegevens in het CRM-systeem en dat men daarin moet kijken;
  - Zorg voor een duidelijke procedure voor het opschonen van het CRM. Als een persoon niet verwijderd kan worden, wis dan alle velden van deze persoon en zet een afgesproken tekst in het veld ‘naam’ zodat je weet dat het om een gewist persoon gaat;
  - Spreek met de derden af (via de verwerkersovereenkomst) dat bestanden voor een eenmalig doel daarna worden verwijderd (bijvoorbeeld het adressenbestand dat aan een drukker wordt aangeboden voor verzending van een mailing);
  - Maak afspraken met je medewerkers en software leveranciers om de gegevens ook echt daadwerkelijk te (kunnen) verwijderen.

4-VERWERKERS-OVEREENKOMSTEN

Verwerkersovereenkomst

- Als organisatie mag je persoonsgegevens niet doorgeven aan een andere partij zonder een **verwerkersovereenkomst**. In een verwerkersovereenkomst spreek je af wat de ander met de gegevens mag doen én ook vooral wat niet.
- Je mag trouwens de gegevens met derden alleen delen als dit noodzakelijk is voor uitvoering van de doeleinden waarvoor je deze hebt verkregen.
- **TIP:** Maak eerst een plaatje/schema van jullie systeemlandschap. Daarmee heb je overzicht over welke verwerkersovereenkomsten er afgesloten moeten worden.

Verwerkersovereenkomst

Belangrijkste bepalingen

- Wie is verantwoordelijke en wie verwerker
- Vertrouwelijkheidsverklaring
- Verbod gegevens te verwerken buiten schriftelijke opdracht
- Adequate beveiliging te realiseren
- Verbod gegevens door te geven, tenzij voor onderaanneming (na goedkeuring)
- Gegevens permanent verwijderen na opdracht (aantoonbaar)
- Meldingsplicht datalek of bijna-datalek
- Verbod zelf te communiceren met autoriteiten of betrokkenen (enkel via verantwoordelijke)
- Auditrecht

Verwerkersovereenkomst

Bijlagen

- Duidelijke omschrijving van de opdracht
  - welke verwerking moet gebeuren
  - Omschrijving van type van gegevens en categorieën van betrokkenen
  - Bewaartermijn van de gegevens
- Beschrijving van de toegepaste beveiligingsmaatregelen
  - informatiebeveiligingsbeleid
  - Eventuele certificaten
- Maatregelen voor beschikbaarheid / Hoe worden data verwijderd
- Afspraken voor melden van datalekken
  - Aangifteformulier
  - Contactgegevens van DPO

5-PROCEDURE ROND DATALEKKEN

Datalekken

- **Wat is een datalek?**

  Een datalek is een inbreuk op de beveiliging van persoonsgegevens. Een datalek is een beveiligingsincident waarbij persoonsgegevens gelekt zijn. Dit kan gaan om een ongeoorloofde toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens. Van een datalek is alleen sprake als er persoonsgegevens zijn gelekt!

Voorbeelden van datalekken:

- Je raakt een USB-stick met daarop persoonsgegevens kwijt.
- Er is een laptop gestolen met daarop persoonsgegevens.
- Er is door een hacker ingebroken in een databestand of systeem (met daarop persoonsgegevens).
- Er is een mailing verstuurd met alle e-mailadressen in de Aan of CC in plaats van BCC.
- Uit een tas zijn papieren gestolen met daarop persoonsgegevens.
- Door een crash van een harddisk of door brand zijn persoonsgegevens verloren gegaan en er is geen back-up.

Datalekken – incident management

- Beperk de impact
  - Foutieve verwerking stoppen (machine of server stilleggen, connectie verbreken…)
  - Datatransfer stoppen (postafgifte tegenhouden, webpagina weghalen, toegang afsluiten, zending terugroepen)
- Analyseer het incident
  - Zijn er persoonsgegevens betrokken? Zo ja, gevoelige of bijzondere? Hoeveel?
  - Is er effectief een datalek? Omvang?
  - Is er impact? Zijn de gegevens versleuteld? Of gepseudonimiseerd?
- Escaleer
  - Persoonsgegevens betrokken?Altijd de DPO inschakelen
  - Ben je verwerker? Altijd de Verantwoordelijke inschakelen
  - Aangifte?
- Bepaal de oorzaak en werk een oplossing uit
- Evalueer en stel verbeterplan op

Datalekken – meldingsplicht

- Incident maar geen datalek
  - Noteer het incident in je interne incidentenlijst
  - Maar een verslag met oorzaak, oplossing, verbeterplan (en opvolging)
  - Rapporteer desgewenst ook aan verantwoordelijke (bijv. in SLA-meeting)
- Datalek maar geen impact
  - Idem EN…
  - Schakel altijd de DPO in
  - Ben je Verwerker? Verwittig (binnen 24u) de Verantwoordelijke
  - Ben je Verantwoordelijke? Geen aangifte nodig (vermeld de gevolgde redenering in je verslag)
- Datalek met (ernstige) impact
  - Ben je Verwerker? Assisteer de Verantwoordelijke – Communiceer nooit zelf
  - Ben je Verantwoordelijke? De DPO doet aangifte binnen 72u
  - Ernstig of niet? Aangifte of niet? DPO adviseert – Noteer altijd de gevolgde redenering
- Datalek met hoog risico op schade
  - Idem EN…
  - Ben je Verantwoordelijke? Contacteer indien mogelijk de betrokkenen

Datalekken – procedure

- Stel een datalek-procedure op
  - Bepaal rollen en verantwoordelijkheden
  - Leg de criteria vast voor escalatie
- Verwerker? Neem contactgegevens van DPO van Verantwoordelijk in je register op
  - Per verantwoordelijke naam en contactgegevens van DPO
  - Per verantwoordelijke type van gegevens
  - Noteer of de verantwoordelijk ook een melding vereist bij bijna-datalek
- Verantwoordelijke? Wat moet je melden?
  - Aard van het incident
  - Type data en type betrokkenen (en zo mogelijk het aantal geïmpacteerden)
  - Reële en mogelijke impact
  - Reeds genomen maatregelen om impact te beperken
  - Contactgegevens van eigen DPO
- Leid personeel op
  - Hoe herken je een incident?
  - Wie moet je verwittigen?

6-VRIJWAREN VAN DE RECHTEN VAN DE BETROKKENE

Rechten van de betrokkene

- Transparantie
  - Informatie over verwerkingen
- Rechten op de eigen gegevens
  - Inzagerecht;
  - recht op rectificatie;
  - recht op vergetelheid;
  - recht op beperking van verwerking;
  - recht op kennisgevingsplicht;
  - recht op overdraagbaarheid van gegevens;
  - recht van bezwaar.

Rechten van de betrokkene - Procedure

- Hoe verloopt een aanvraag?
  - Betrokkenen moeten de juiste werkwijze makkelijk kunnen vinden
  - Interne medewerkers moeten vragen kunnen kanaliseren
  - Vlotte doorstroming moet zorgen voor tijdige afhandeling (30 dagen)
- Hoe moet een verzoek afgehandeld worden?
  - Werk uit welke info waar te vinden is
  - Leg criteria vast voor ingaan op verzoeken of niet
  - Stel een standaard motivering op voor afwijzingen
- Hoe volg je op?
  - Hou een actielijst bij van verzoeken, antwoorden en motivaties (en status)
  - Evalueer het proces en stel verbeterplannen op

7-BEWUSTMAKING VAN DE MEDEWERKERS

Informeer medewerkers over hun plichten

Wat wordt van jou als medewerker verwacht?

- Ondertekenen de geheimhoudingsverklaring (deze kan al deel zijn van je arbeidsovereenkomst);
- Houd je aan de regels van jullie privacy policy;
- Gebruik de persoonsgegevens alleen voor het doel waarvoor ze zijn afgegeven;
- Versnipper documenten met persoonsgegevens als deze niet meer bewaard hoeven te worden;
- Geef nooit persoonsgegevens aan derden zonder verwerkersovereenkomst;
- Sla nooit persoonsgegevens op op servers of online diensten buiten de EU;
- Zorg ervoor dat je computer en virussoftware up-to-date zijn en blijven

Geef medewerkers praktische richtlijnen

Onderstaande punten gelden voor iedereen binnen je organisatie.

Tip: maak een (geplastificeerde) kaart met deze praktische tips en leg die op elke werkplek:

- Blokkeer altijd je scherm als je je werkplek verlaat;
- Laat documenten met persoonsgegevens nooit onbeheerd achter op je bureau of op de printer;
- Kies nooit voor automatisch opslaan van inloggegevens op je computer;
- Besef dat openbare netwerken niet veilig zijn;
- Let op wat je deelt via sociale media;
- Bedek altijd je webcam om 'meekijken' te voorkomen;
- Gebruik nooit de inlog van een collega en geef je inloggegevens ook niet door aan een collega;
- Zorg ervoor dat je mobiele telefoon beveiligd is met een wachtwoord (inlogcode)

Procedure – Opleiding personeel

- Organiseer een introductieopleiding voor nieuwe medewerkers
- Herhaal minstens elk jaar de training
- Gebruik affiches of infoborden om tips te geven
- Stel een brochure op
- Organiseer eens een oefening of een quiz
- Vergeet ook interims, tijdelijke medewerkers, consultants niet

8-COMPLIANT ZIJN

Wat maakt je GDPR-compliant?

- Wij beschikken over een **dataregister**
- Ons **privacybeleid** werd aangepast
- De nodige **technische en organisatorische maatregelen** werden getroffen ter bescherming van de persoonsgegevens
- We hebben u een **verwerkersovereenkomst** gestuurd waarbij duidelijk gestipuleerd staat voor welke doeleinden we de persoonsgegevens gaan gebruiken.
- De **verantwoordelijke voor data privacy** binnen onze organisatie is: xxxx
- Wij hebben een procedure die duidelijk vastlegt wat er moet gebeuren bij **een datalek**
- Wij hebben een regeling om ervoor te zorgen dat wij **de rechten van de betrokkenen** kunnen garanderen
- Ons personeel is **op de hoogte van het belang van de GDPR** en van de interne procedures en wettelijke verplichtingen, vooral van het feit dat persoonsgegevens vertrouwelijk zijn en beschermd

Kun je het ook aantonen?

- Heb je voldoende kennis in huis?
  - Heeft de DPO/Verantwoordelijke een attest van zijn opleiding?
  - Heb je lijsten (en evaluaties) bijgehouden van deelnemers aan een interne opleiding?
- Is vastgelegd welk doel en welke rechtsgrond elke verwerking heeft?
- Heb je de risico's van de verwerking gewogen en je beveiliging daarop afgestemd?
  - Beschik je over een beschrijving van je risicoanalyse?
  - Wanneer is deze het laatst geactualiseerd? Welk actieplan is toen opgesteld?
- Kun je aantonen dat je je beveiliging controleert en dat de maatregelen afdoend zijn?
- Heb je een intern register van incidenten (en datalekken), met evaluatie?
- Heb je als verantwoordelijke controle over verwerkers?
  - Verslag van screening / Verwerkersovereenkomst / Evaluatie van de leverancier
- Leg je vast hoe je elk verzoek van een betrokkene hebt afgehandeld?

Om af te sluiten….

- **De GDPR/AVG is een uitgebreide en gecompliceerde wettekst.**
- Dit stappenplan is een **sterk gecomprimeerde uitleg en interpretatie** hiervan. Wij kunnen niet garanderen dat deze informatie altijd volledig juist, compleet en actueel is.
- De gegeven informatie is dan ook uitsluitend bedoeld als **algemene informatie** en hier kunnen verder geen rechten aan worden ontleend.
- Deze informatie kan helpen om een **beter beeld te krijgen van de privacyregelgeving** en het vormgeven en uitvoeren van je privacy policy.
- Het kan **niet** worden opgevat als een concreet juridisch advies.
- Leidend blijft de officiële wettekst GDPR/AVG.

KEEP CALM AND COMPLY WITH GDPR

FEBELGRA - AGALLIS

BNP PARIBAS FORTIS

Agallis INSURANCE SERVICES

febelgra united in graphics

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

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
Boom, 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