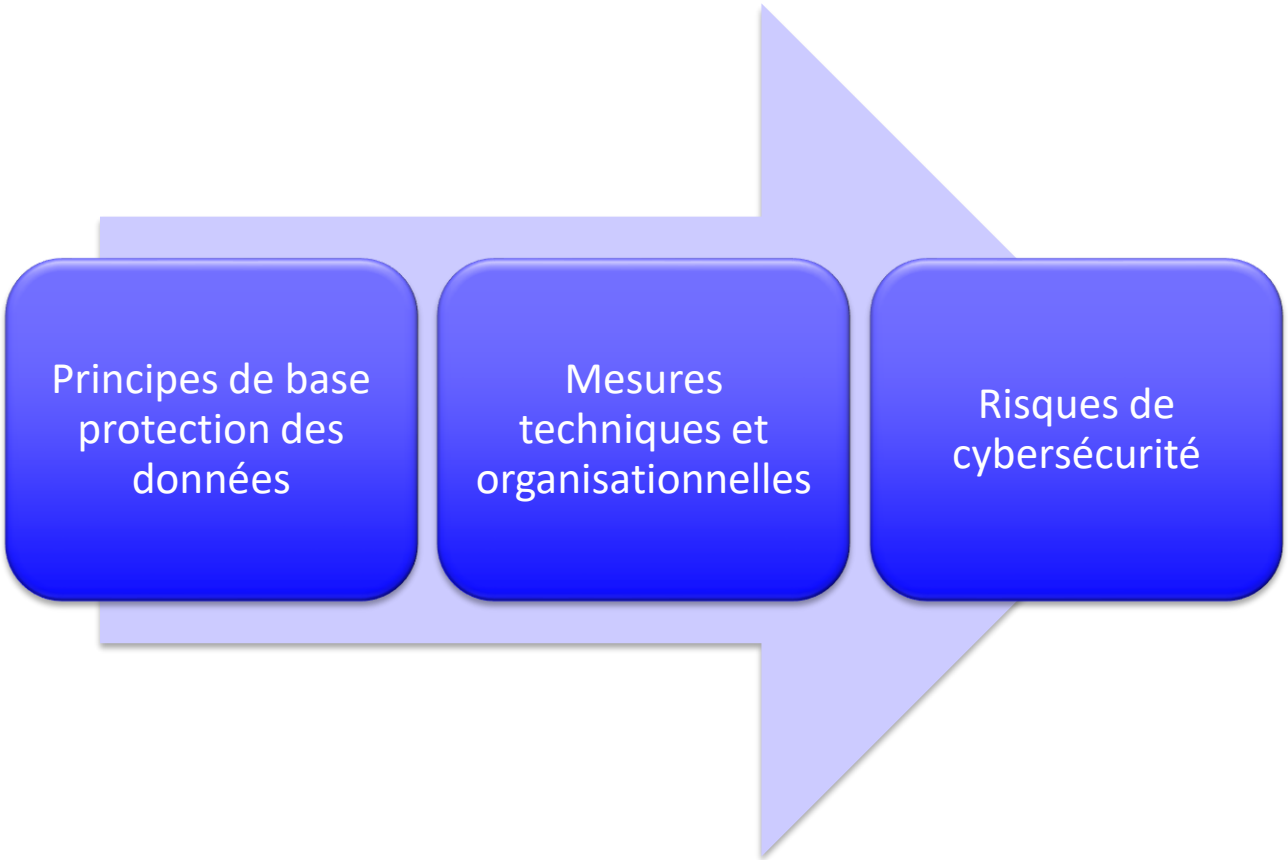
Protection des données et risques de cybersécurité dans le secteur de la santé



Embracing technology
Embracing ambition

.AGORIA

Programme


Principes de base protection des données
Mesures techniques et organisationnelles
Risques de cybersécurité

.AGORIA

Cyberattaque à l'hôpital d'Armentières: 300.000 patients concernés par le vol de données

Publié le 28/02 à 17h34 par AFP

L'attaque, survenue dans la nuit du 10 au 11 février, avait été confirmée "par l'impression de plusieurs messages de ransomware sur les imprimantes de l'établissement", avait indiqué le centre hospitalier le jour-même.

L'établissement avait dû fermer temporairement ses urgences à la suite de cette cyberattaque.

Incidents dans le secteur de la santé?

.AGORIA

Tentative de cyberattaque : le CHC MontLégia toujours en "phase rouge"

22 févr. 2023 à 12:27· 1 min
Par Martial Giot

Le 18 novembre dernier, le Groupe santé CHC avait détecté une intrusion suspecte dans son système informatique. Le groupe hospitalier liégeois avait immédiatement pris des mesures préventives de protection. Toutes les connexions vers l'extérieur avaient été coupées. Elles le sont toujours.

Pour les patients, une conséquence très pratique du confinement de son système informatique est l'impossibilité d'introduire en ligne une demande de rendez-vous. Depuis trois mois, ils se prennent uniquement par téléphone. Par ailleurs, les médecins généralistes n'ont plus accès au portail web qui leur est, en temps normal, destiné.

rtbf actus

Incidenten in de zorgsector ?

.AGORIA

7 juni 2023

Zorgsector goed voor 41% van alle datalekken

In totaal spelen 41% van de datalekken in Nederland zich af in de ziekenhuizen en aanverwante organisaties. Daarmee is de zorg de meest gehackte sector van Nederland. Dit blijkt uit de begin juni 2023 gepresenteerde datalekkenrapportage 2022 van de Autoriteit Persoonsgegevens. Het is niet toevallig dat juist bijvoorbeeld ziekenhuizen zo vaak slachtoffer van cybercriminelen zijn, want data uit medische dossiers zijn wereldwijd goede handel.

De afgelopen vijf jaar ontving AP meer dan 114.000 datalekmeldingen. Ook in 2022 was er weer een groot aantal meldingen over datalekken, in totaal 21.151. Meer dan 1.800 lekken waren het gevolg van cyberaanvallen, die extra gevaarlijk zijn. AP-voorzitter Aleid Wolfsen licht toe: "Dit overzicht laat overduidelijk zien dat datalekken een hardnekkig probleem zijn. Reden te meer voor de AP om te waarschuwen voor de gevaren van datalekken, en om iedereen op het hart te drukken om serieus werk te maken van de bescherming van persoonsgegevens. Ook jij kunt slachtoffer worden, ook al denk je misschien van niet."

Medisch dossier is geld waard

Laurentius Ziekenhuis informeert patiënten over datalek

Een medewerker van het Laurentius Ziekenhuis in Roermond heeft de medische dossiers van 95 patiënten ingezien terwijl hij daar niet bevoegd voor was. Gedupeerde patiënten zijn daarvan op de hoogte gebracht. Het Limburgse ziekenhuis heeft tevens maatregelen genomen om herhaling in de toekomst te voorkomen.

VPN Gids 17 november 2022

Belgisch ziekenhuis AZ Herentals meldt datalek

Het AZ Herentals-ziekenhuis in de Belgische provincie Antwerpen meldt een datalek. Een 'onbekende entiteit' kreeg volgens het ziekenhuis ongeoorloofd toegang tot een aantal documenten tijdens een 'cyberincident'.

Nieuwsblad

Gegevens van 150.000 Belgische ziekenhuispatiënten gelekt

21 maart 2022

Datalek ASZ: half miljoen medische bestanden overschreven

Er was geen opzet bij, maar het Albert Schweitzer ziekenhuis zijn van zo'n 212.000 patiënten een of meer digitale documenten verloren gegaan. Dat gebeurde doordat de betreffende bestanden overschreven werden door nieuwere documenten. Volgens het ASZ zijn door deze fout met name verwijsbrieven, onderzoeksresultaten of aantekeningen van de behandelaar verwijderd. In totaal gingen meer dan een half miljoen documenten verloren.

.AGORIA

Principes de base protection des données

1. Data Protection by Design & by Default
2. Responsabilité
3. Confidentialité
4. Minimisation des données

Data Protection by Design & by Default ?

.AGORIA

Data Protection by Design / Protection des données dès la conception

- Prévoir les garanties nécessaires
- Lors de la mise en œuvre du traitement
- Lors de la création de programmes ou d'applications
  - Pour respecter les prescriptions
  - Pour protéger les droits des personnes concernées

➢ Data Protection by Default / Protection des données par défaut

- Offrir un niveau de protection maximal compte tenu du risque
  - Échelle
  - Délai
  - Accessibilité

Qu'est-ce que les données à caractère personnel ?

.AGORIA

Données à caractère personnel

- Toute information
- Identifiée ou identifiable
- Individu (= **personne concernée**)
- Identifiant

Données non personnelles

- Données ne pouvant pas être reliées à un individu
  - Organisation
  - Produits
  - Services

~~RGPD~~

RGPD

nom

âge

adresse

profession

adresse IP

formation

photo

GPS

santé

condamnation

conviction

Qu'est-ce qu'une catégorie particulière de données à caractère personnel ?

.AGORIA

➔ Également dénommées **données** sensibles

- origine raciale ou ethnique
- opinions politiques
- convictions religieuses ou philosophiques
- appartenance syndicale
- **données génétiques ou biométriques permettant d'identifier une personne physique de manière unique ou données concernant la santé**
- données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

Interdiction de traitement ➔ 11 exceptions

Que sont les données personnelles pseudonymisées / cryptées ?

.AGORIA

traitement de données à caractère personnel de telle façon que celles-ci

- ne puissent plus être attribuées à une personne concernée précise
- sans avoir recours à des informations supplémentaires
- pour autant que ces informations supplémentaires soient conservées séparément
- soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne soient pas attribuées à une personne physique identifiée ou identifiable

Quels principes à suivre?

Quels principes à suivre?

.AGORIA

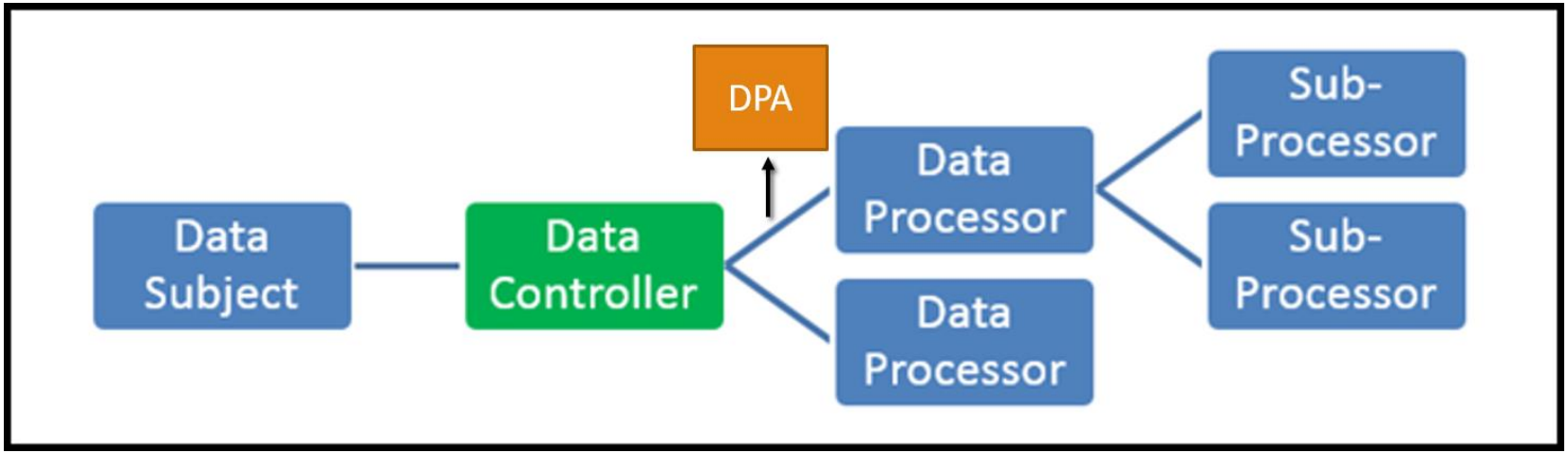
Responsable du traitement

- Démontrer la conformité
  - ❑ analyse des risques
  - ❑ documenter (preuve)
    - Registre
    - Notes d'information
    - Procédures
    - Décision
  - ❑ trainings & awareness

Qui est le responsable du traitement (data controller) ?

.AGORIA

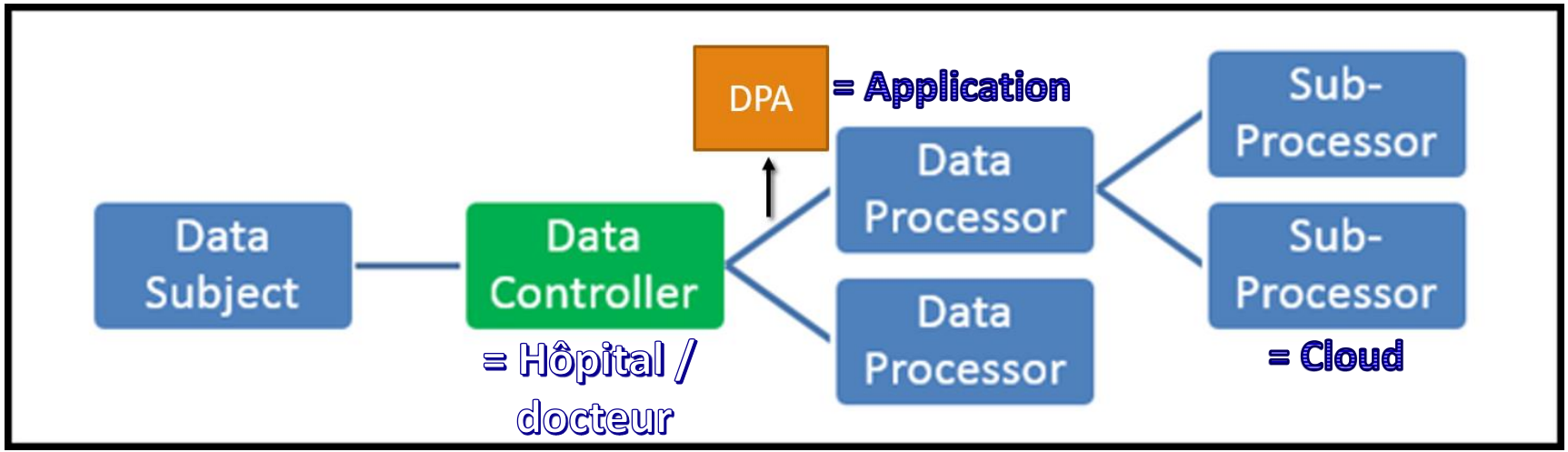
Natuurlijke persoon (individu) of rechtspersoon (organisatie), overheidsinstantie die het **doel** en de **middelen** voor de verwerking van persoonsgegevens vaststelt



Qui est le responsable du traitement (data controller) ?

.AGORIA

Personne physique (individu) ou personne morale (organisation), autorité publique qui détermine **les finalités** et **les moyens** du traitement des données à caractère personnel



Quels principes à suivre?

Confidentialité (faire respecter) ?

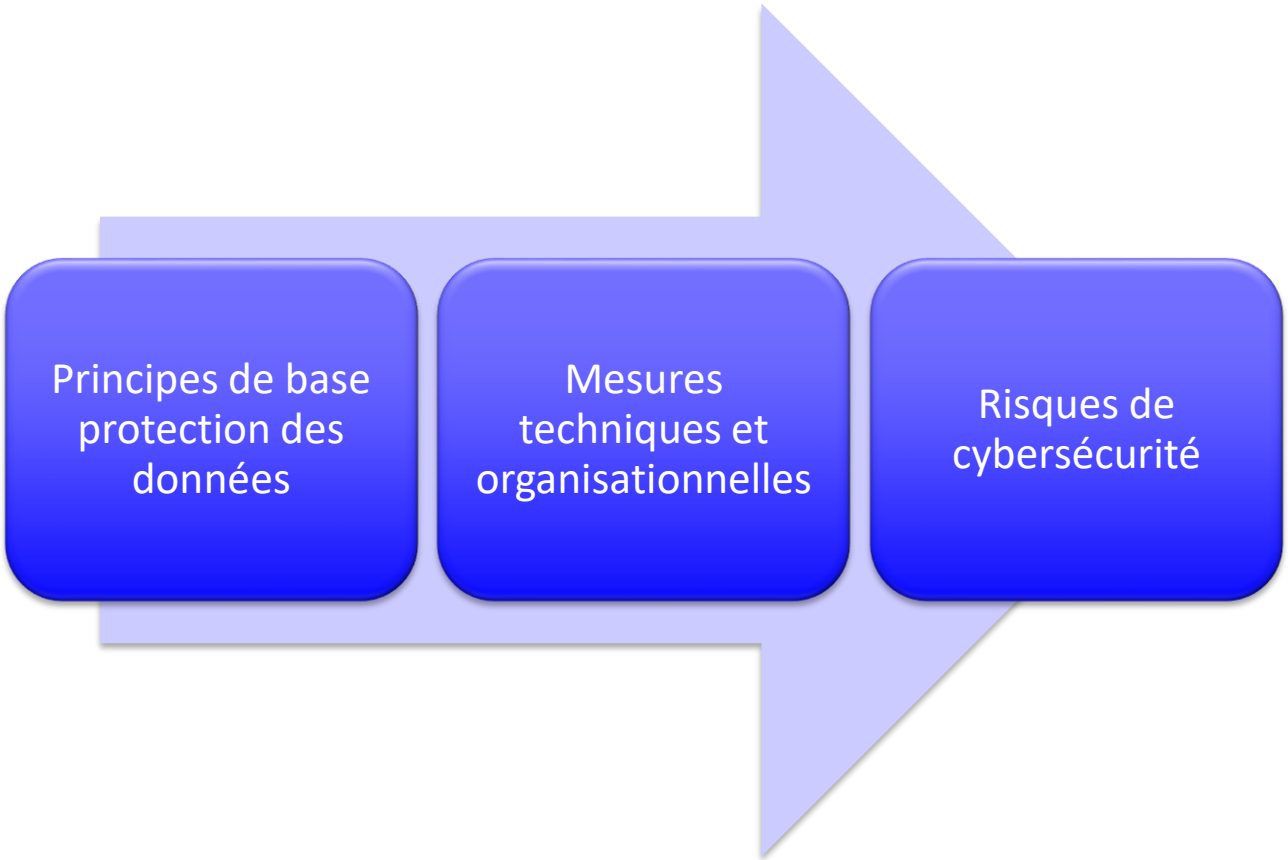
.AGORIA

- ✓ Accès aux données à caractère personnel
  - ➢ Need-to-know : Déterminer qui a accès aux données
  - ➢ Software-applications (screenings, assessments, …)
    - Déterminer les droits d'accès au server / tool
    - Protéger les parties du serveur / tool
    - Redéfinir les droits d'accès (p. ex., changement de fonction)

- ✓ Awareness
  - ➢ Sensibilisation à la protection des données et à l'importance de la confidentialité et de l'intégrité
  - ➢ Préciser au sein de l'entreprise ce qui est permis et ce qui ne l'est pas

- ✓ Obligation de confidentialité
  - ➢ Contrat de travail
  - ➢ Règlement de travail

Programme


Principes de base protection des données
Mesures techniques et organisationnelles
Risques de cybersécurité

Programme

.AGORIA

Risques de cybersécurité

1. Système informatiques/logiciels dépassés
2. Phising & ransomware
3. Pas de réseau wifi verrouillé/séparé dans le cabinet
4. Pas de (up-to-date) firewall, antivirus, …
5. 1 login pour plusieurs utilisateurs
6. Back-ups ⇔ cloud
7. Envoi de données à caractère personnel par e-mail
8. Mots de passe faibles
9. Gestion de l'accès et des droits
10. Sensibilisation - Awareness

1. Système informatique / logiciels dépassés

.AGORIA

► Par ses deux délibérations en date du 7 décembre 2020, la formation restreinte de la CNIL inflige deux amendes de 3 000 euros et 6 000 euros à l'encontre de deux médecins libéraux pour avoir insuffisamment protégé les données personnelles de leurs patients et ne pas avoir notifié une violation de données à la CNIL conformément au « RGPD » (Règlement n° 2016/679 du 27 avril 2016).

Faits et procédure. À la suite d'un contrôle en ligne réalisé en septembre 2019, la CNIL a constaté que des milliers d'images médicales hébergées sur des serveurs appartenant à deux médecins libéraux étaient librement accessibles sur internet.

Lors des auditions de contrôle, les médecins ont reconnu que les violations de données avaient pour origine un mauvais choix de configuration de leur box internet ainsi qu'un mauvais paramétrage de leur logiciel d'imagerie médicale. Les investigations menées ont également permis d'établir que les images médicales conservées sur leurs serveurs n'étaient pas systématiquement chiffrées.

1. Système informatique / logiciels dépassés

.AGORIA

Des départements informatiques manquant de ressources : les pénuries de personnel et les restrictions budgétaires touchent tous les services de l'hôpital, ce qui peut conduire à ce que des éléments comme les correctifs de sécurité passent à travers les mailles du filet et à ce que les piles technologiques ne soient pas mises à jour et renforcées pour répondre aux demandes et aux risques modernes. En outre, le HHS signale que l'hôpital type est tout simplement « dépassé » par les cyberattaquants du point de vue de la technologie et du personnel.

1. Système informatique / logiciels dépassés

.AGORIA

Pour entrer dans le système informatique d'un hôpital, ils emploient plusieurs voies possibles. *"Soit ils vont profiter d'une vulnérabilité dans le système informatique, soit ils utilisent des techniques d'ingénierie sociale, ou encore une combinaison des deux"*, explique Michele Rignanese, porte-parole du Centre pour la Cybersécurité belge (CCB). Une vulnérabilité, c'est une porte d'accès facile pour un hacker.

Nicolas van Zeebroek distingue trois raisons qui expliquent pourquoi les hôpitaux sont des cibles privilégiées des pirates informatiques.

"La première, c'est que les hôpitaux possèdent des données extrêmement sensibles. C'est donc très problématique si les données sont inaccessibles, ou pire, si elles fuitent dans la nature, ce qui est souvent la menace que profèrent ces attaquants."

"D'autre part, les hôpitaux ont besoin de leur système de manière impérative. Il y a des vies qui sont en danger derrière, il y a des soins impératifs à donner. Et donc bloquer un hôpital est extrêmement critique. Il faut donc réagir très vite."

"Troisièmement, les hôpitaux sont souvent un peu sous-investis en informatique, et donc pas toujours en mesure de parer parfaitement à ce type d'attaque."

1. Système informatique / logiciels dépassés

.AGORIA

"We will share your sensitive data with the public, if you don't cooperate": het is een voorbeeld van wat ransomware slachtoffers te zien krijgen wanneer hun computer is gegijzeld. Als er één plek is waar een ransomware aanval grote gevolgen heeft, dan is het wel de zorgsector. Inmiddels zijn in Nederland de meeste meldingen van datalekken afkomstig uit de zorg. Wat zijn de consequenties als privacygevoelige data van de patiënt op straat komt te liggen? En is er wat tegen te doen?

Het is oktober 2020 als tienduizenden Finnen een email ontvangen waarin staat dat hun medische data publiekelijk online verschijnt als ze niet binnen 24 uur €200,- in bitcoin betalen. Bij het missen van de eerste deadline, moest er binnen 48 uur €500,- betaald worden. De hackers hebben een lek ontdekt bij het Finse psychotherapiecentrum Vastaamo en maken zich meester van medische dossiers. De buitgemaakte data bestaat uit de volledige namen van patiënten, hun sofinummers, de naam van de kliniek waar ze zijn behandeld en de transcripties van therapiesessies.

afhankelijke it-systemen

De zorgsector blijft de meest kwetsbare sector als het om data-incidenten gaat. Waarom? In tegenstelling tot bijvoorbeeld de financiële sector gebruiken veel zorgaanbieders nog steeds gedateerde systemen. Daarnaast wordt steeds meer medische apparatuur met het internet verbonden. Er is natuurlijk ook de afhankelijkheid van externe hardware en software uit het buitenland. Vorige maand nog kreeg de Amerikaanse softwareleverancier Kaseya te maken met ransomware op de ICT-beheersoftware. Deze software wordt door meer dan 40.000 bedrijven wereldwijd gebruikt. Uiteindelijk leken slechts een paar

2. Phising & Ransomware

.AGORIA

7 juni 2023

Zorgsector goed voor 41% van alle datalekken

In totaal spelen 41% van de datalekken in Nederland zich af in de ziekenhuizen en aanverwante organisaties. Daarmee is de zorg de meest gehackte sector van Nederland. Dit blijkt uit de begin juni 2023 gepresenteerde datalekkenrapportage 2022 van de Autoriteit Persoonsgegevens. Het is niet toevallig dat juist bijvoorbeeld ziekenhuizen zo vaak slachtoffer van cybercriminelen zijn, want data uit medische dossiers zijn wereldwijd goede handel.

De afgelopen vijf jaar ontving AP meer dan 114.000 datalekmeldingen. Ook in 2022 was er weer een groot aantal meldingen over datalekken, in totaal 21.151. Meer dan 1.800 lekken waren het gevolg van cyberaanvallen, die extra gevaarlijk zijn. AP-voorzitter Aleid Wolfsen licht toe: “Dit overzicht laat overduidelijk zien dat datalekken een hardnekkig probleem zijn. Reden te meer voor de AP om te waarschuwen voor de gevaren van datalekken, en om iedereen op het hart te drukken om serieus werk te maken van de bescherming van persoonsgegevens. Ook jij kunt slachtoffer worden, ook al denk je misschien van niet.”

Medisch dossier is geld waard

Datalekken en oplichting

Uit Amerikaans onderzoek blijkt dat een compleet medisch dossier, met verzekeringsnummer, adres en BSN tussen 50 en 500 dollar kan opbrengen. Dat is veel meer dan bijvoorbeeld een creditcardnummer, dat op de zwarte virtuele markt nog geen euro waard is. Niet vreemd, want een patiëntendossier biedt niet alleen meer informatie, maar ook veel meer mogelijkheden. Denk alleen maar eens aan verzekeringsfraude of het stelen van recepten voor bepaalde medicijnen. Cybercriminelen gebruiken buitgemaakte gegevens, zoals e-mailadressen, namen en andere persoonlijke informatie, ook om grote groepen mensen en organisaties op te lichten met nepberichten die afkomstig lijken van betrouwbare instanties.

2. Phising & Ransomware

.AGORIA

En effet, ces informations valent dix fois plus que les renseignements sur les cartes de crédit. Il n'est donc pas surprenant que les hôpitaux se trouvent dans la ligne de mire des cybercriminels. Même un petit hôpital peut contenir des informations sensibles sur plus de 100 000 personnes. Si un pirate informatique arrive à accéder à un réseau hospitalier, c'est donc une véritable aubaine pour lui.

les violations dans le secteur de la santé ont atteint un niveau record en 2021, poursuivant une tendance à la hausse qui a vu le nombre de dossiers médicaux américains violés plus que tripler au cours des trois dernières années. Les dossiers de santé sont une cible populaire pour une raison simple : les dossiers médicaux valent jusqu'à 40 fois plus que les données de cartes de crédit volées sur le dark web. En effet, les dossiers médicaux contiennent généralement des informations allant du numéro de sécurité sociale aux informations sur les bénéficiaires des régimes de santé, voire des identifiants biométriques, sans compter les informations sur les comptes financiers.

.AGORIA

Les hôpitaux bruxellois font l'objet de cyberattaques

Les mails, la porte d'entrée

Différents moyens existent pour contourner la sécurité d'un hôpital : *« L'une des méthodes la plus utilisée par les hackers est de se faire passer pour un docteur et de modifier l'adresse mail. Ils ajoutent une pièce jointe qui contient des éléments qui permettent de diffuser un malware dans le système d'un hôpital. En échange d'une rançon, ils proposent de donner la clé de déchiffrement. »*

Les deux plus grands types d'attaques lucratives contre les hôpitaux sont l'extraction de données de santé et les ransomwares. A cela, s'ajoute la complexité de tout sécuriser au sein de l'institution avec l'augmentation de l'utilisation des objets connectés (monitoring, médecine, appli...) qui peut ouvrir une voie d'entrée pour différents piratages. Pour l'hôpital, tout cela a évidemment un coût. Ce dernier est souvent gardé secret pour ne pas donner des informations aux hackers mais il n'est pas pris en charge actuellement par le budget des soins de santé. L'argent sort donc directement de la poche de l'hôpital.

.AGORIA

Gezondheidsgegevens van ggz-patiënten Pro Persona zijn gestolen door phishing

Een ggz-instelling in Gelderland is getroffen door een phishingaanval. Criminelen kregen daardoor toegang tot de mailboxen van vier medewerkers, waarin ook gezondheidsgegevens over cliënten stonden.

Het gaat om de ggz-instelling Pro Persona. Die bevestigt tegenover RTL Nieuws dat het last had van een datalek, nadat het medium daar een melding over had gekregen. Pro Persona stuurde de afgelopen tijd een waarschuwing naar patiënten. Het zou gaan om enkele honderden patiënten van de instelling waarvan hun persoonlijke gezondheidsinformatie mogelijk is gelekt. De organisatie zegt tegen RTL dat er geen aanwijzingen zijn dat de data is misbruikt.

In januari werden er meerdere phishingmails naar instellingen van Pro Persona gestuurd. Vier medewerkers klikten daarbij op een link waardoor zij naar een pagina werden geleid waar zij hun inloggegevens invulden. Daardoor hadden de criminelen zeker één nacht toegang tot de inboxen van de medewerkers. In de inboxen waren naast de namen, adressen en geboortedatums ook gegevens over de gezondheid van patiënten te vinden. Volgens een woordvoerder zou de schade 'zeer beperkt' zijn en was het door technische maatregelen mogelijk 'snel te acteren'. De organisatie heeft een melding gedaan bij de Autoriteit Persoonsgegevens, wat verplicht is bij een dergelijk datalek.

3. Pas de reseau wifi vérouillé/séparé dans le cabinet

.AGORIA

L'environnement WiFi des hôpitaux est une mine d'or potentielle pour les cybercriminels

Le nombre croissant d'appareils sans fil qui sont maintenant utilisés dans les hôpitaux incite davantage les pirates informatiques à tenter d'accéder à leurs réseaux WiFi.

Non seulement les médecins utilisent des téléphones mobiles pour s'y connecter et communiquer des renseignements médicaux personnels, mais il y a aussi des ordinateurs portables et un nombre croissant d'appareils médicaux connectés à ces réseaux. Ceci augmente le risque d'attaques cybercriminelles.

De plus, les patients peuvent se connecter à ces réseaux WiFi, tout comme les visiteurs, et ils ont aussi besoin d'être protégés contre de nombreuses menaces, dont voici quelques-unes :

Les hôpitaux bruxellois font l'objet de cyberattaques

Il veille sur toutes les portes d'entrée à risque : « On sensibilise les employés. On a 10.000 personnes sur le site et 6.000 employés. Ils nous préviennent lorsqu'il y a un couac et on prend les mesures. On a, à ce jour, jamais eu de données médicales à risque piratées. Elles sont fortement protégées. » Le département informatique de Saint-Luc est composé de 60 personnes : « Face à une attaque, notre plus grand défi est de permettre aux patients d'être soignés et à l'hôpital de fonctionner. On sépare nos réseaux. Le réseau public ne permet pas d'entrer dans le réseau de l'hôpital. »

3. Pas de reseau wifi vérouillé/séparé dans le cabinet

.AGORIA

Nieuwsblad

Gegevens van 150.000 Belgische ziekenhuispatiënten gelekt

In ons land werden de Emmaüs-ziekenhuizen van Duffel en Malle getroffen door het datalek. In Nederland ging het om het St. Anna Ziekenhuis in Geldrop en het Canisius-Wilhelmina Ziekenhuis in Nijmegen. Van de ruim 200.000 gelekte dossiers komen er ruim 195.000 uit België.

Het lek kwam er na een 'menselijke fout' bij het Belgische IT-bedrijf iGuana, dat oude patiëntendossiers digitaliseert. Om de medische informatie uit te wisselen werd gebruik gemaakt van een onbeveiligde webserver en internetlink. Ongeveer een maand lang waren de gegevens van de patiënten (hun dossiernummer, naam, geslacht, geboortedatum) zomaar toegankelijk voor iedereen.

4. Pas de (up-to-date) firewall, antivirus, …

.AGORIA

Antivirus = Prevention !

- Analyse ordinateur
- Identifie les dangers
- Elimine les dangers

➔Monitoring

➔ Mises à jour !

- automatiquement
- tous les postes de travail / appareils
- serveur

Firewall = agent de sécurité

Login et mot de pass ne suffisent pas

Firewalls et routeurs sécurisés empêchent les intrus d'accéder au réseau

Idéalement intégrés à l'antivirus

.AGORIA

Toegangsbeperking en controle voor gebruik medische gegevens

Wat opvalt is dat in de medische sector, veel boetes worden uitgeschreven wegens een te laks toegangsbeleid. Zo wordt meermaals benadrukt dat niet meer personen mogen toegang hebben tot de medische gegevens dan nodig. Zo werd een ziekenhuis in Portugal veroordeeld tot een boete van 400.000 euro onder andere omdat iedere dokter toegang had tot alle patiëntengegevens, ongeacht zijn specialiteit. Dat de software niet of een afwijking hierin was voorzien werd niet als een verzachtende omstandigheid aangenomen.

Tevens wordt erop gewezen dat controle (logging) moet worden uitgevoerd of mogelijk zijn op alle personen die toegang hebben tot gevoelige persoonsgegevens om te kunnen controleren of zij geen misbruik maken van hun bevoegdheid. Een zorgverzekeraar in Nederland werd hiertoe veroordeeld tot een bedrag van 50.000 euro.

6. Back-ups ⇔ cloud

.AGORIA

Back-ups

- Eviter de perdre toutes les données
- Fréquance ?
- Sécurité back-up(s) ?
- Risque que la sauvegarde (back-up) elle-même soit infectée

Cloud Back-up

- Automatisé / régulier
- plusieurs back-ups
- Sécurité = up-to-date
- Partenaire cloud fiable

7. Envoi de données à caractère personnel par e-mail

.AGORIA

40. Comme cela ressort des articles précités, le responsable du traitement est obligé de mettre en œuvre les mesures techniques et organisationnelles nécessaires afin de garantir que le traitement de données s'effectue conformément au RGPD. Les hôpitaux dont la tâche principale consiste à prodiguer des soins médicaux traitent régulièrement de grandes quantités de données de santé. Ils doivent donc être particulièrement vigilants et veiller à ce que ces données soient traitées conformément au RGPD. La Chambre Contentieuse souligne que les données à caractère personnel relatives à la santé (et la transmission de celles-ci) doivent être suffisamment sécurisées et que les données doivent dès lors être envoyées sous une forme présentant un niveau de cryptage suffisamment élevé au départ de l'ordinateur de l'utilisateur vers le serveur qui propose un site Internet avec un formulaire. Cela peut se faire en utilisant un certificat de sécurité.

.AGORIA

Gezondheidsgegevens van ggz-patiënten Pro Persona zijn gestolen door phishing

Een ggz-instelling in Gelderland is getroffen door een phishingaanval. Criminelen kregen daardoor toegang tot de mailboxen van vier medewerkers, waarin ook gezondheidsgegevens over cliënten stonden.

Het gaat om de ggz-instelling Pro Persona. Die bevestigt tegenover RTL Nieuws dat het last had van een datalek, nadat het medium daar een melding over had gekregen. Pro Persona stuurde de afgelopen tijd een waarschuwing naar patiënten. Het zou gaan om enkele honderden patiënten van de instelling waarvan hun persoonlijke gezondheidsinformatie mogelijk is gelekt. De organisatie zegt tegen RTL dat er geen aanwijzingen zijn dat de data is misbruikt.

In januari werden er meerdere phishingmails naar instellingen van Pro Persona gestuurd. Vier medewerkers klikten daarbij op een link waardoor zij naar een pagina werden geleid waar zij hun inloggegevens invulden. Daardoor hadden de criminelen zeker één nacht toegang tot de inboxen van de medewerkers. In de inboxen waren naast de namen, adressen en geboortedatums ook gegevens over de gezondheid van patiënten te vinden. Volgens een woordvoerder zou de schade 'zeer beperkt' zijn en was het door technische maatregelen mogelijk 'snel te acteren'. De organisatie heeft een melding gedaan bij de Autoriteit Persoonsgegevens, wat verplicht is bij een dergelijk datalek.

7. Envoi de données à caractère personnel par e-mail

.AGORIA

Meldingen datalekken uit zorg stijgen

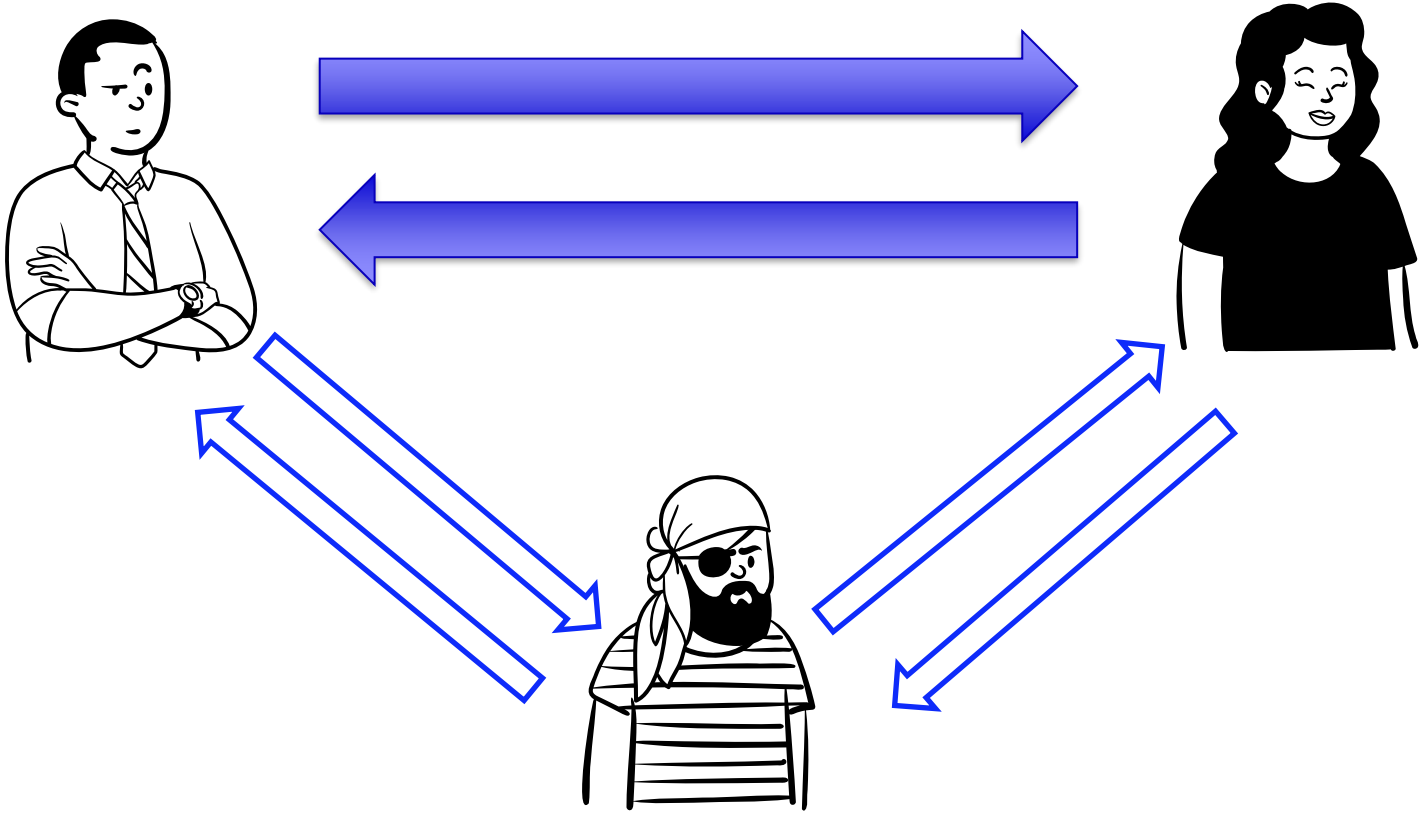
Plaats een reactie

Het aantal meldingen van datalekken dat de Autoriteit Persoonsgegevens in 2017 kreeg, is flink gestegen ten opzichte van 2016. Dat geldt voor het totaal aantal meldingen, maar ook specifiek voor de hoofdleverancier van lekken: de zorg. Relatief neemt het aandeel meldingen uit de zorg niet toe.

Wat betreft de zorg gaat het in 60 procent van de gemelde datalekken om persoonsgegevens die aan de verkeerde ontvanger zijn verstuurd of afgegeven. In slechts 3 procent van de gevallen ging het om hacking, malware of phishing. Het soort gelekte gegevens betrof meestal naam-, adres- en woonplaatsgegevens en/of personalia (geslacht, leeftijd, geboortedatum), maar in driekwart van de gevallen werden (ook) gezondheidsgegevens gelekt. Ziekenhuizen en specialistenpraktijken waren de voornaamste melders (772 meldingen).

7. Envoi de données à caractère personnel par e-mail

.AGORIA



.AGORIA

Onderzoek

Naar aanleiding van de melding van het HagaZiekenhuis heeft de AP een nader onderzoek ingesteld en aan het ziekenhuis in april 2019 een voornemen toegezonden tot het opleggen van een bestuurlijke boete en/of een last onder dwangsom. Na een zienswijze van het HagaZiekenhuis en een zienswijzezitting bij de AP heeft de AP geoordeeld dat de overtreding voortduurt en heeft besloten tot het opleggen van de boete.

Onder artikel 32, eerste lid, AVG is de verwerkingsverantwoordelijke bij de verwerking van persoonsgegevens gehouden tot het nemen van "passende technische en organisatorische maatregelen" ter beveiliging van de gegevens. Volgens de AP is het HagaZiekenhuis hierin op twee verschillende onderdelen tekortgeschoten: (i) het ziekenhuis had regelmatig moeten controleren welke werknemer welk dossier raadpleegt en monitorde onvoldoende de logbestanden om onbevoegde inzage te achterhalen en (ii) het ziekenhuis had de identiteit van medewerkers door middel van een tweefactor authenticatie moeten vaststellen, waardoor er niet conform het eigen autorisatiebeleid is gehandeld. Hiermee overtreedt het ziekenhuis niet alleen de AVG, maar ook de relevante zorgwetgeving en de voor de zorgsector geldende NEN7510-2 normen voor informatiebeveiliging.

De AP lijkt de enige toezichthouder in Europa te zijn met een concreet en volledig uitgewerkt boetebeleid. Op grond van dit boetebeleid, en gelet op de (opzettelijke of nalatige) aard, ernst en duur van de inbreuk, het feit dat er bijzondere persoonsgegevens bij het datalek betrokken waren, en de door het ziekenhuis genomen maatregelen, komt de toezichthouder uit op een boete ter hoogte van € 460.000,-. Hiernaast verbeurt het ziekenhuis een dwangsom van €100.000,- per twee weken dat de overtreding voortduurt, met een maximum van €300.000,- wanneer de beveiliging niet vóór 2 oktober 2019 op orde is gebracht.

8. Mots de passe faibles

.AGORIA

L'adresse mail et le mot de passe ont été divulgés?

➔ Modifiez votre mot de passe dès que possible!

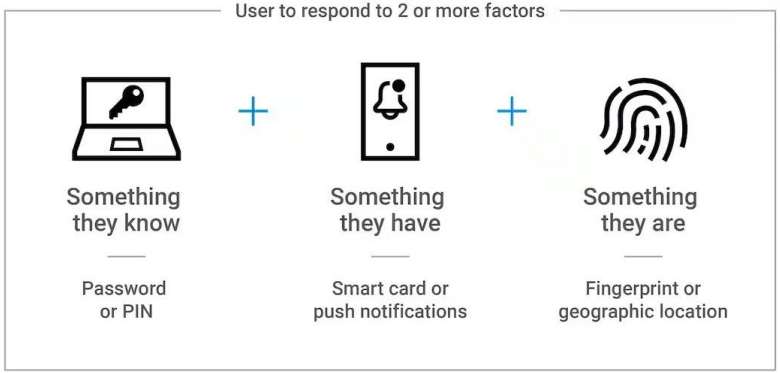
1 compte / login = 1 mot de pass

Mot de pass fort

- ✓ 14 caractères
- ✓ Complex

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
18	9 months	23m years	6tn years	100 tn years	7qd years



9. Gestion de l'accès et des droits d'accès

.AGORIA

« Entre le 3 janvier 2019 et le 4 janvier 2019, le Dr Y1 à eu accès à mon insu à mon dossier médical en ligne alors que je ne suis plus patiente depuis 2017, ce dernier a eu accès à mon dossier médical en ligne via le réseau santé wallon et ce à 214 reprises, il a tout imprimé. […] Ce dernier crée un lien thérapeutique abusif alors que je n'ai plus rien à voir avec lui » (plainte du 6 novembre 2019)

> *« la tenue d'un dossier médical pour chaque patient est imposée par la loi coordonnée sur les hôpitaux et les autres établissements de soins et l'arrêté royal du 3 mai 1999 déterminant les conditions générales minimales auxquelles le dossier médical, visé à l'article 15 de la loi sur les hôpitaux, coordonnées le 7 août 1987, doit répondre ;*
> *Le fonctionnement même de l'hôpital exige que chaque médecin puisse avoir accès au dossier du patient dans le cadre d'une hospitalisation (service des urgences, service des soins intensifs, laboratoire, etc)…[…]*
> *Il nous est donc impossible, et à l'encontre de l'économie même du fonctionnement d'un hôpital, de n'autoriser l'accès au dossier médical qu'à certains professionnels. En effet, chaque médecin de notre institution peut être amené à soigner un patient et donc à consulter son dossier médical. La traçabilité nous permet néanmoins de vérifier que chaque professionnel de soins de santé respecte ses obligations. Nous effectuons d'ailleurs pour ce faire des coups de sonde occasionnellement ».*

9. Gestion de l'accès et des droits d'accès

.AGORIA

The DPA launched its investigation after a tip from a concerned member of the public, reports in the media and two notifications of data breaches by OLVG about work placement students and other staff accessing medical records even though it was not necessary for their work. After its investigation, the DPA concluded that there are structural shortcomings in the way OLVG secures access to medical records. Specifically, it found two violations of data protection law:

- Every time a staff member accesses medical records, these details must be recorded in a log. In addition, the hospital must review this access log regularly, so that it can take timely steps if it finds that someone has accessed a record when they are not actually authorised to do so. OLVG did have an automated procedure that logged who accessed which files, but it did not review the logs often enough to check for cases of unauthorised access.
- Good security requires two-factor authentication to establish the identity of a user who wants access to a patient record. Examples are a code or password in combination with a personnel badge. OLVG did not require two-factor authentication when access was requested from inside the hospital. Access from a location outside the hospital was secured with two-factor authentication.

.AGORIA

Accès aux données médicales d’une personne par un médecin chargé d’évaluer son état de santé : rappel à l'ordre

25 février 2020 par PM

L'actualité récente a fait état de consultations illégales de dossiers médicaux électroniques par des médecins. L'Ordre rappelle que le réseau d'accès électronique permettant l'accès aux données de santé d'une personne par les praticiens ayant une relation thérapeutique avec celle-ci ne peut pas être utilisé par le médecin chargé d'une mission d'expertise .

.AGORIA

Secretaresse Bravis Ziekenhuis bekeek 347 keer dossier van patiënt

Het Laurentius Ziekenhuis is niet de enige zorginstelling waar het recentelijk mis ging. In het Bravis Ziekenhuis in Roosendaal raadpleegde een voormalige medewerkster 347 keer het patiëntendossier van de ex-vrouw van haar partner. De oud-secretaresse verwerkte de medische gegevens in een boek dat ze schreef over de vechtscheiding van haar partner.

Toen de patiënt het boek van de oud-medewerkster onder ogen kreeg, waarschuwde ze het Bravis Ziekenhuis. Die constateerde dat de voormalige secretaresse in vier jaar tijd honderden keren had bekeken, terwijl ze daar niet bevoegd voor was. Daarop spande de patiënt een rechtszaak aan tegen het ziekenhuis. Zij eiste een schadevergoeding van 15.000 euro voor immateriële schade, een verhuiskostenvergoeding van 20.000 euro en compensatie van 3.000 euro voor de beveiliging van haar huis.

De rechtbank erkende dat er sprake was van inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer, maar vond een schadevergoeding van 2.000 euro beter passen bij de overtreding.

.AGORIA

Laurentius Ziekenhuis informeert patiënten over datalek

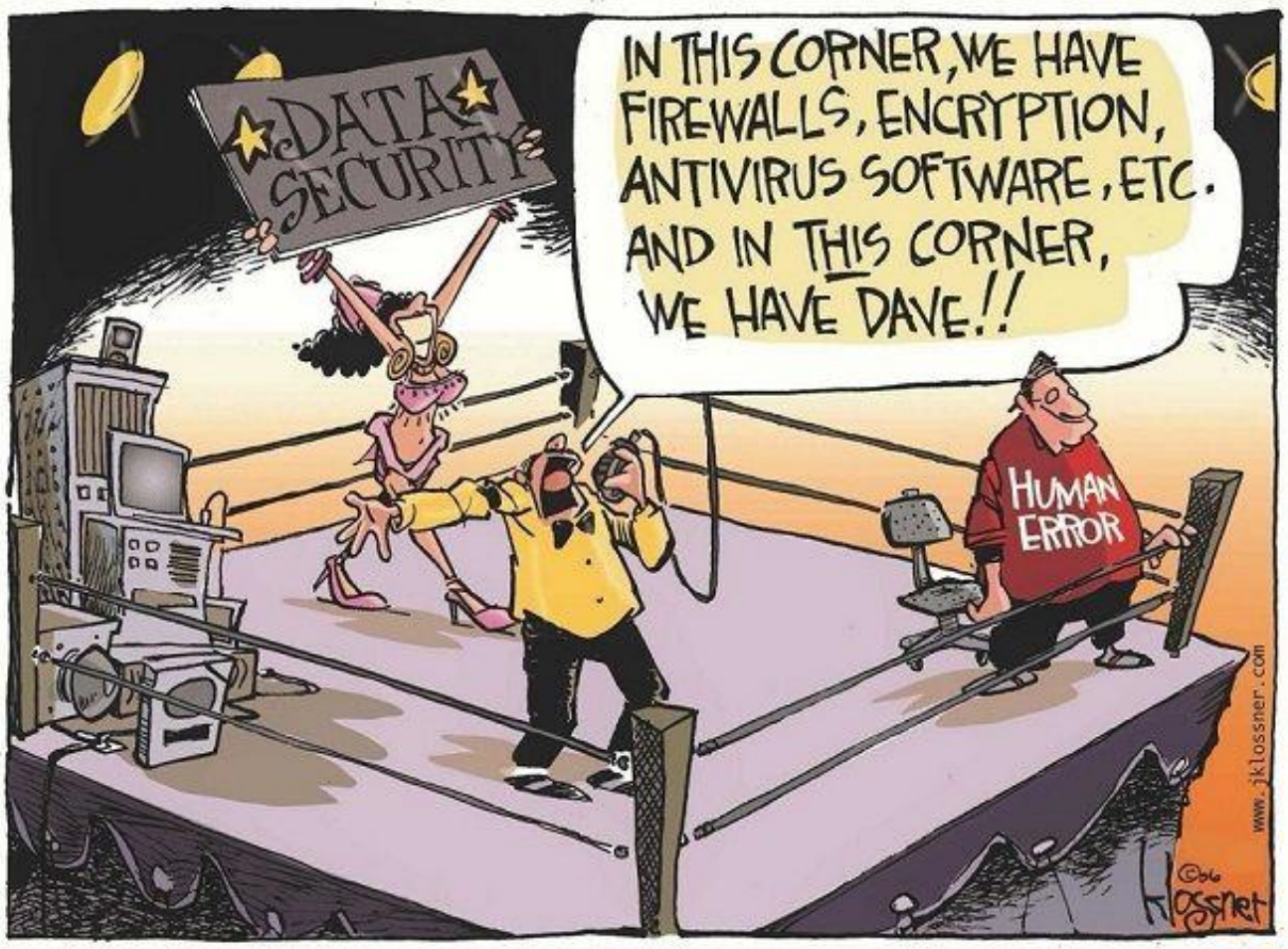
Een medewerker van het Laurentius Ziekenhuis in Roermond heeft de medische dossiers van 95 patiënten ingezien terwijl hij daar niet bevoegd voor was. Gedupeerde patiënten zijn daarvan op de hoogte gebracht. Het Limburgse ziekenhuis heeft tevens maatregelen genomen om herhaling in de toekomst te voorkomen.

VPN Gids 17 november 2022

Het voorval kwam aan het licht toen een zorgmedewerker zag dat een collega door de dossiers van ziekenhuispatiënten bladerde. Toen hij dit merkte heeft hij dit doorgegeven aan het ziekenhuis. Volgens het Laurentius Ziekenhuis heeft de betreffende medewerker “in de afgelopen periode” de medische dossiers van 95 patiënten bekeken. Er is geen reden om aan te nemen dat de werknemer persoonsgegevens heeft gedeeld met een ander, maar wel dat hij er misbruik van heeft

10. Sensibilisation / Awareness

.AGORIA



.AGORIA

Les hôpitaux bruxellois font l'objet de cyberattaques

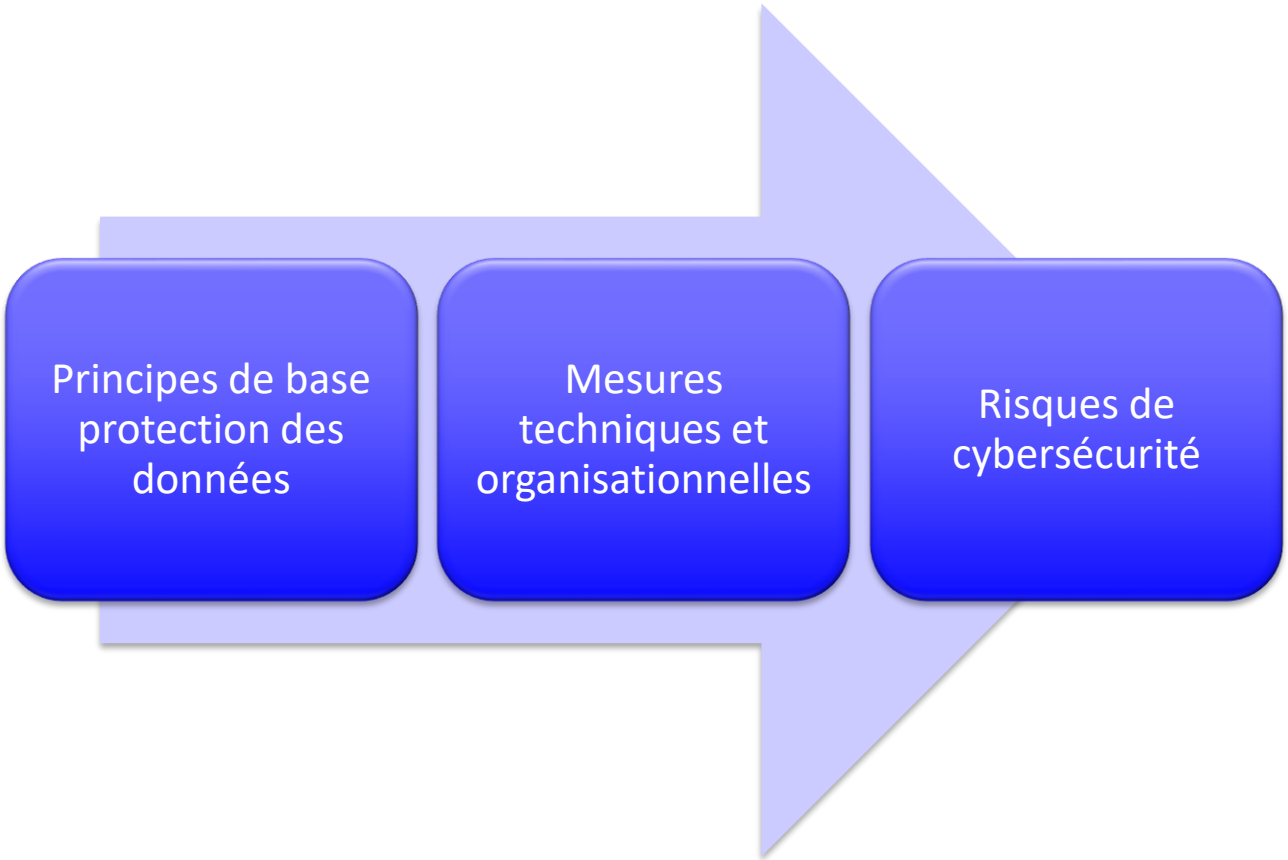
Il veille sur toutes les portes d'entrée à risque : « On sensibilise les employés. On a 10.000 personnes sur le site et 6.000 employés. Ils nous préviennent lorsqu'il y a un couac et on prend les mesures. On a, à ce jour, jamais eu de données médicales à risque piratées. Elles sont fortement protégées. » Le département informatique de Saint-Luc est composé de 60 personnes : « Face à une attaque, notre plus grand défi est de permettre aux patients d'être soignés et à l'hôpital de fonctionner. On sépare nos réseaux. Le réseau public ne permet pas d'entrer dans le réseau de l'hôpital. »

S'entraîner

Au Chirec aussi, des mesures sont prises comme dans d'autres institutions et une sensibilisation à un personnel très varié (personnel administratif, médical, infirmière, médecin...) est constante au travers de plans ciblés ou d'entraînements avec des faux phishing.

Dans d'autres hôpitaux bruxellois, une fois par an, des scénarios à risque sont lancés par des consultants externes pour tester le système. Ces entraînements permettent de voir les failles dans les différentes composantes de l'hôpital et de les sécuriser après.

Programme


Principes de base protection des données
Mesures techniques et organisationnelles
Risques de cybersécurité

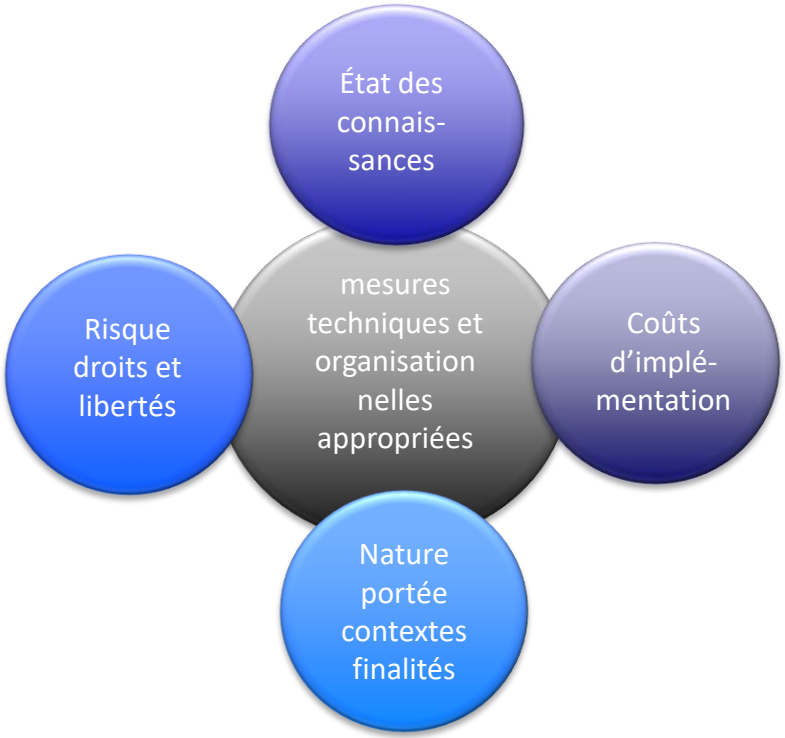
.AGORIA

Mesures techniques et organisationnelles

1. Prévenir les risques / violations
2. Atténuer les conséquences de toute infraction
3. Sensibilisation
4. Notification des violations de données

Comment déterminer et appliquer les mesures de sécurité appropriées ?

.AGORIA



❑ Equilibre : risk based approach

- Risques
  - ➢ Analyse des risques (loi) :
    - Catégories particulières de données
    - Évaluation systématique
    - Surveillance lieux publics
  - ➢ Risque de violation de données
  - ➢ Analyse préventive des risques dans le cadre de sécurité-vulnérabilité
  - ➢ Analyse préventive des risques dans le cadre de risk-based approach
    - probabilité
    - gravité

➔ **Prévenir les infractions et les fuites de donnée**

Comment déterminer et appliquer les mesures de sécurité appropriées ?

.AGORIA

- pseudonymisation et chiffrement
- moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement
- moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique
- procédure visant à analyser et à évaluer régulièrement l'efficacité des mesures de sécurité
- application d'un code de conduite approuvé
  - les codes contribuent à l'application correcte du GDPR
  - compte tenu des nécessités spécifiques pour certains secteurs
  - besoins PME
- application d'un mécanisme de certification approuvé
- confidentialité travailleurs
  - need-to-know

Comment déterminer et appliquer les mesures de sécurité appropriées ?

.AGORIA

Juridique

- Obligation de confidentialité
- Contrat de sous-traitant
- Clauses contractuelles types / BCR (règles d'entreprise contraignantes) / …

Awareness

- Formations et/ou séances d'information
- Répétition
- Code de conduite
- Directives (policy, alerts, …)

Physique

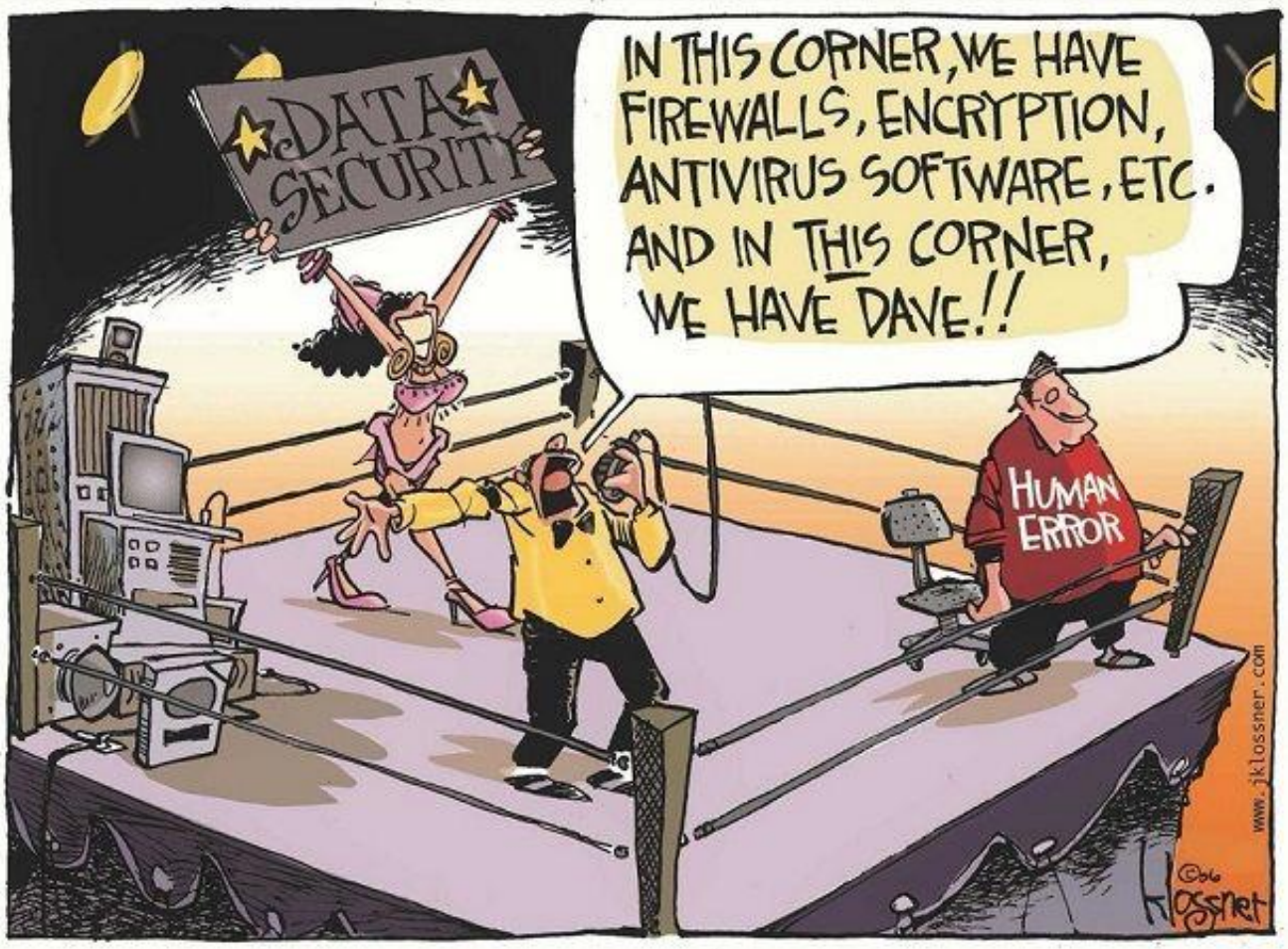
- Accès sécurisé
- Protection contre l'eau/l'incendie/…

Mesures techniques

- Droits d'accès
- Mots de passe
- Protection de l'appareillage
- Cryptographie
- Sauvegarde
- Logiciel malveillant
- Protection du réseau

Comment déterminer et appliquer les mesures de sécurité appropriées ?

.AGORIA



Violaton des données : Pas si, mais quand cela arrivera-t-il ?

.AGORIA

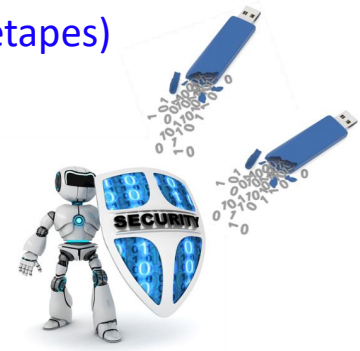
- **Accidentelle**
- **Illicite**
  - Destruction
  - Perte
  - Altération
  - Divulgation non autorisée
  - Accès non autorisé

- **Plupart des violations sont ‘accidentelles’ (en interne !)**

.AGORIA

- Notification violation de données à l'Autorité de Protection des Données
  - Si risque pour les droits et libertés de l'individu
  - Dans les 72 heures après en avoir pris connaissance (retard : motifs + par étapes)

> **Manquement à l'obligation de notifier les violations de données à la CNIL (« RGPD », art. 33).** La formation restreinte a également retenu un manquement à l'obligation de notifier les violations de données à la CNIL.



- Contenu notification
  - Nature de la violation
    - Catégories de personnes concernées
    - Catégories de données à caractère personnel
    - Nombre de personnes concernées
  - Nom et coordonnées DPO (ou autre point de contact)
  - Conséquences de la violation
  - Mesures pour atténuer les conséquences négatives

Contrôle compliance

Violaton des données : Pas si, mais quand cela arrivera-t-il ?

.AGORIA

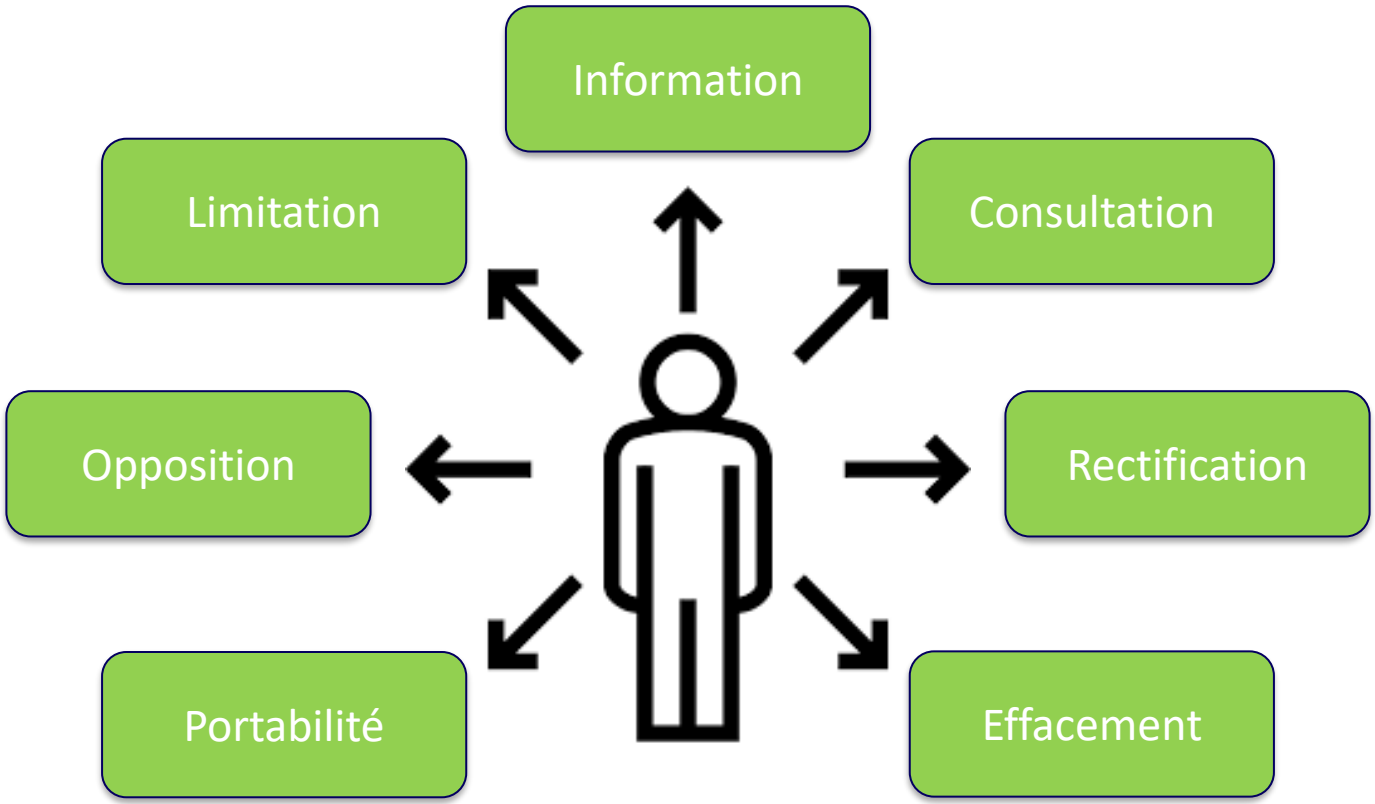
- Notification violation de données à l'individu
  - Si risque élevé pour les droits et libertés de l'individu

  Non requis : efforts disproportionnés (communication publique) ; chiffrement ; risque élevé ne se produira plus

- Obligation de notification sous-traitant à responsable du traitement

- **Documenter** chaque violation
  - Faits
  - Conséquences
  - Mesures correctrices

Incident de sécurité et droits du patient concerné ?



.AGORIA

- faciliter l'exercice des droits
- procédures permettant d'accéder à l'exercice des droits en temps voulu (dans un délai d'un mois)
- Informer les destinataires de l'exercice des droits
- introduire des procédures automatisées
- Avec quel support transmettre des données (preuve) ?
- Quel format pour transmettre des données ?

Incident de sécurité et sanctions?

.AGORIA

En l'espèce, la Chambre contentieuse décide qu'une page web permettant aux médecins de consulter à distance les résultats d'analyses médicales de patients sans offrir de chiffrement, **viole le principe d'intégrité et de confidentialité inscrit aux articles 5.1.f) à l'article 32 du RGPD**.

PAR CES MOTIFS,

la Chambre Contentieuse de l'Autorité de protection des données décide, après délibération:

- en vertu des articles 100,§1°,13° et 101 de la LCA, **d'imposer une amende de 20.000 EUR pour la violations des articles 5.1.f), 12, 13, 14, 32, 35.1 et 35.3 du RGPD**

Incident de sécurité et sanctions?

.AGORIA

The Dutch Data Protection Authority (DPA) has imposed a fine of €440,000 on the Amsterdam-based hospital OLVG for its inadequate protection of patients' medical records. Between 2018 and 2020 OLVG did not have sufficient safeguards in place to prevent unauthorised access to the records. It did not carry out proper checks of who accessed which records, and there were shortcomings in information systems security. In response to the DPA's investigation OLVG has made the required improvements.

Embracing technology
Embracing ambition

Thank you

For your attention

Thomas Van Gremberghe

thomas.vangremberghe@agoria.be

.AGORIA