BACHELORPROEF

Wat is de impact van de General Data Protection Regulation (GDPR) op de IT-processen van een internationale onderneming?

Research bij Kinepolis Group NV

Kinepolis Group NV
Gent

Bachelor	Toegepaste Informatica
Keuzetraject	Computer & Cyber Crime Professional
Academiejaar	2017-2018
Student	Kevin Bollengier
Interne begeleider	Bjorn Van Reet
Externe promotor	Koen Cornelis & Johan Galle

howest.be

Woord vooraf

Om mijn opleiding Toegepaste Informatica met specialisatie Computer & Cybercrime Professional af te sluiten, kreeg ik de kans om stage te lopen in een snelgroeiende onderneming namelijk Kinepolis Group NV. De hoofdzetel (Headquarters), waar ik mijn stage heb uitgevoerd is gelegen in Gent.

Naar aanleiding van “Secure your future”, een evenement georganiseerd in samenspraak met Howest, Kinepolis, Intigriti en The Security Factory, kreeg ik de kans om de CIO van Kinepolis te ontmoeten. Na deze ontmoeting mocht ik er in de zomer aan de slag gaan om mee te helpen bouwen aan het securityverhaal binnen Kinepolis als vakantiejob.

Het onderwerp van mijn stage en bachelor proef mocht ik zelf kiezen van Bjorn. Ik besloot om mij te verdiepen in de “General Data Protection Regulation” of GDPR in het kort. Het is mijn taak om samen met het GDPR-team binnen Kinepolis de technische uitwerking van deze nieuwe regelgeving uit te voeren.

Ook wil ik enkele personen bedanken die me tot op het einde steunden om mijn doel te bereiken. Allereerst de personen die het evenement “Secure your future” hebben georganiseerd, dankzij jullie evenement sta ik waar ik nu sta. Vervolgens wens ik ook Bjorn Van Reet te bedanken, voor het vertrouwen, de mogelijkheden die je voor me openstelde en de unieke kans om me te laten specialiseren als Data Protection Officer. Ik wil ook alle collega’s binnen Kinepolis bedanken omdat zij steeds bereid waren om mij te ondersteunen telkens het nodig was.

Ik wil ook de externe medewerkers van Kinepolis bedanken voor hun steun tijdens mijn stageproject met in het bijzonder Pommeline Steegmans van PwC en Frederik Ringoot van DLA Piper voor de suggesties die ze mij gaven en die ik heb opgenomen in deze bachelor proef.

Door het onderwerp van mijn bachelor proef kreeg ik ook de kans om staatssecretaris van privacy Philippe De Backer te interviewen. Ik wil hem bedanken voor de tijd en de unieke kans om dit te realiseren.

Daarnaast wil ik ook de leerkrachten van Howest en in het bijzonder de leerkrachten van de DPO-opleiding bedanken om altijd open te staan om vragen in verband met GDPR te beantwoorden.

Tot slotte ook een bedankje naar Koen Cornelis en Johan Galle, mijn interne promotoren, vanwege de ondersteuning van mijn stage en het geven van feedback wanneer deze nodig was.

Samenvatting

We leven in een digitaliserende en snel evoluerende wereld op vlak van informatica. Bij digitalisering behoren natuurlijk veel data waaronder ook persoonlijke data.

Voor het ontstaan van GDPR had elke lidstaat van de Europese Unie reeds richtlijnen en wetgeving inzake databescherming, maar deze kon per lidstaat verschillen. GDPR vervangt deze richtlijnen om ze te uniformiseren voor alle lidstaten van de Europese Unie. Ook zorgt GDPR er nu voor dat meer soorten data als persoonlijke data gezien worden. Elk bedrijf dat klantendata verwerkt en bijhoudt van Europese burgers is onderworpen aan de GDPR.

Het doel van mijn onderzoek is bekijken welke impact de GDPR heeft op verschillende vakgebieden binnen informatica zoals security, privacy en big data. Een ander doel van het onderzoek is bekijken hoe de totstandkoming van compliance aan de GDPR binnen een onderneming aangepakt dient te worden.

Sleutelwoorden: GDPR, security, databescherming, technische aanpak.

Abstract

We live in a digitalizing and rapidly evolving world in the field of information technologies. With digitization, there is of course a lot of data involved, including personal data.

Prior to GDPR, each Member State of the European Union already had directives and legislations on data protection. These, could however differ per Member State. GDPR aims to replace these guidelines to align them for each Member State of the European Union. GDPR also covers more data which previously was not considered as personal data. Also with GDPR, every company which processes and/or maintains customer data from European citizens is subject to this new legislation.

The aim of my research is to examine the impact of GDPR on various fields within IT such as security, privacy and big data. Another aim of the research is to examine how compliance towards GDPR is established within a company.

Keywords: GDPR, security, data protection, technical approach.

Verklarende woordenlijst

BEGRIP	DEFINITIE
GDPR	General Data Protection Regulation of in het Nederlands, Algemene Verordening inzake Gegevensbescherming. Dit is de nieuwe Europese verordening die nageleefd moet worden bij het verwerken van persoonsgegevens.(Zie hoofdstuk "Wat is de General Data Protection Regulation?")
DPO	Data Protection Officer (Functionaris voor Gegevensbescherming), de verantwoordelijke die aangesteld wordt om raad te geven, te informeren en te adviseren in verband met het beschermen van gegevens.
ENISA	European Network and Information Security Agency. Dit is het Europees expertisecentrum inzake cyber security.
DATA SUBJECT	Een natuurlijke persoon die kan geïdentificeerd worden.
CONTROLLER	Organisatie of onderneming die data verzamelt over data subjects die verblijven binnen de Europese Unie, ook wel de verwerkingsverantwoordelijke genoemd.
PROCESSOR	Organisatie die data verwerkt in opdracht van een data controller, ook wel de verwerker genoemd.
PERSOONSGEGEVENS	Elke informatie van een geïdentificeerde of direct of indirect kan leiden tot het identificeren van een data subject.
PROCESSING/VERWERKING VAN PERSOONSDATA	Dit is elke handeling die uitgevoerd op persoonlijke data zoals het verzamelen, opnemen, organiseren, structureren, opslaan, etc..
PROFILING	Elke vorm van geautomatiseerde verwerking van persoonsgegevens om bepaalde persoonlijke voorkeuren te analyseren of te voospellen.
REPURPOSING	Data verwerken voor een ander doel dan het origineel bepaalde doel.
DATA MINIMALISATION	Enkel de noodzakelijke gegevens mogen gevraagd worden.
RECHTSGEVOLG	Een gevolg van een rechtshandeling (bv: afsluiten van een overeenkomst)
TOKENIZATION	Een niet-wiskundige oplossing voor het vervangen van gevoelige gegevens.

VERORDENING	Een wetgevend instrument van een bepaalde overheidsinstantie, ook wel een wetgevende akte.
JOINT-CONTROLLERS	Dit is een relatie van controllers/verwerkingsverantwoordelijken waarbij de betrokken controllers samen doel en middel van de verwerking opstellen.
BIG DATA	Dit is de verzamelterm van grote datasets die geanalyseerd worden met computers om trends, patronen te ontdekken, meestal gerelateerd aan menselijk gedrag.
PSEUDONIMISATION	Pseudonimisatie is een techniek waarbij de identificeerbare velden van persoonsgegevens vervangen wordt. Dit is een methode om “privacy by design” te implementeren.
GEGEVENSBESCHERMINSGAUTORITEIT	Dit is de autoriteit die instaat voor de bescherming van persoonlijke gegevens, ze staat in voor de controle of gegevens al dan niet correct gebruikt worden. Deze instantie is dan ook bevoegd voor audits en indien nodig sancties op te leggen. Voor België was deze instantie voorheen gekend als de privacy commisie.

Inhoudsopgave

1 Voorstelling van het bedrijf

De Kinepolis Group ontstond in 1997 uit de fusie van twee familiale bioscoopgroepen en is sinds 1998 beursgenoteerd. Kinepolis staat voor een innovatief bioscoopconcept dat als baanbrekend geldt binnen de sector en stelt alles in het werk om haar bezoekers de 'ultieme filmbeleving' te bezorgen.

Kinepolis Group telt diverse bioscopen in België, Frankrijk, Nederland, Luxemburg, Spanje, Zwitserland, Polen en Canada. Naast haar activiteit als bioscoopuitbater is de Kinepolis Group ook actief in filmdistributie, events, schermreclame en vastgoedbeheer.

1.1 Missie en strategie

Kinepolis Group wil voor haar klanten, medewerkers, aandeelhouders, partners en omgeving duurzame waarden creëren. De drie pijlers van haar strategisch model gaan daarbij samen met duurzaam ondernemerschap.

Kinepolis wil de beste cinema-operator zijn

Kinepolis wil bezoekers laten genieten van unieke ontspanningsmogelijkheden en zakelijke ervaringen in de best mogelijke omstandigheden. Kinepolis streeft hierbij naar een technische en logistieke topkwaliteit hetgeen resulteert in een unieke bioscoopbeleving.

Kinepolis wil de beste marketeer zijn

Door een intensieve interactie met haar bezoekers en een aanbod op maat, wil Kinepolis maximaal tegemoetkomen aan de behoeften en wensen van haar publiek. Door in te spelen op het verwachtingspatroon van diverse doelgroepen wil Kinepolis zich profileren als beste marketeer.

Kinepolis wil de beste vastgoedmanager zijn

Kinepolis wil haar unieke vastgoedportefeuille optimaal beheren, valoriseren en verder ontwikkelen.

Alle pijlers staan in het teken van het creëren van "The Ultimate Movie Experience", een bioscoopconcept waarbij de totaalbeleving van de bezoeker centraal staat. Kinepolis zag haar inspanningen hiertoe beloond met een 'Global Achievement in Exhibition Award' in 2014, een erkenning als beste bioscoopuitbater ter wereld.

1.2 Het Kinepolis concept

Kinepolis zet in op klantgerichte innovatie met onder andere relatiemarketing en actieve programmatie. Deze drang naar vernieuwing leidt tot snelle digitalisering van de bioscoop. Kinepolis profileert zich als filmexpert en gebruikt deze kennis om in te spelen op de voorkeuren van haar bezoekers, een resultaat hiervan is actieve programmatie. Hierbij maakt Kinepolis keuzes welke films er per bioscoopcomplex gespeeld worden.

1.3 Onderdelen van de Kinepolis Group

De Kinepolis Group bestaat uit 5 delen:

Bioscoopuitbater

Dit is de kernactiviteit van Kinepolis. Deze activiteit bestaat uit zowel het verkopen van bioscooptickets. Als de “In-Theatre Sales”, waar onder andere alle verkopen van dranken en snacks in bioscoopcomplexen onder vallen.

Business-to-Business

Sinds de digitalisering en dankzij geavanceerde en flexibele infrastructuur kan Kinepolis zich profileren als de ideale partner voor congressen, avant-premières en bedrijfsevenementen.

Brightfish

Bij de overname van Brightfish in 2011 zorgde Kinepolis voor een stabiele partner in schermreclame binnen de bioscoopsector. Brightfish biedt een brede waaier aan mediakanalen aan voor iedereen die wil communiceren met de bioscoopbezoeker.

Kinepolis Film Distribution (KFD)

KFD legt zich specifiek toe op de distributie van nationale en internationale films. Via KFD verzorgt Kinepolis als mediabedrijf ook de distributie en promotie van de Vlaamse films.

Kinepolis Real Estate

Kinepolis onderscheidt zich van veel andere bioscoopuitbaters door haar unieke vastgoedpositie. De Kinepolis Group heeft namelijk het overgrote deel van haar vastgoed in eigen handen en verhuurt ook heel wat ruimte aan derden.

1.4 Enkele cijfers

- Kinepolis heeft ongeveer 3750 werknemers.
- Kinepolis haalde in 2016 een brutowinst van 100 209 000 EUR
- In 2016 waren er 23,8 miljoen bioscoopbezoekers
- Op dit moment worden er 93 bioscoopcomplexen uitgebaat door Kinepolis
- In die 93 complexen zijn er 814 bioscoopzalen
- In deze 814 zalen zijn er in totaal 180 291 plaatsen

1.5 De toekomstvisie van Kinepolis

Kinepolis wil blijven innoveren en investeren om de meerwaarde van het concept van de “Ultimate Movie Experience” te blijven aanbieden aan de klant. Verder wil Kinepolis ook blijven investeren in een kwalitatief filmaanbod in combinatie met verdere expansie van het Kinepolis concept. Kinepolis gelooft ook in het idee van “human capital”, waardoor investeren in medewerkers een van de absolute prioriteiten is.

2 Onderzoeksvraag

Wat is de impact van de GDPR op de IT-processen van een internationale onderneming?

In deze onderzoeksvraag worden volgende deelvragen bekeken:

- *Wat is de GDPR?*
- *Welke gevolgen heeft de GDPR voor de betrokkenen?*
- *Welke plichten heeft een verwerkingsverantwoordelijke?*
- *Wat bij gegevensverwerking door een externe processor?*
- *Welke gevolgen heeft GDPR op IT Governance?*
- *Wat zijn de gevolgen van GDPR op IT Security?*
- *Wat zijn de gevolgen van GDPR op IT-development?*

Ik koos voor deze onderzoeksvraag omdat ik ervan overtuigt ben dat IT-security, IT governance en gegevensbescherming naast elkaar horen te staan om de beste resultaten te boeken binnen een onderneming voor een sterk IT-securitybeleid. Door deze onderzoeksvraag te kiezen kon ik mijzelf verdiepen in de impact die de GDPR heeft op de verschillende vakgebieden van IT en kon ik research doen naar de juridische kant van GDPR.

Om deze vraag te beantwoorden zal ik deze verder uitsplitsen naargelang gerelateerde onderwerpen aan GDPR die bijdragen aan een algemene verhoging van de security en compliance binnen een onderneming.

3 Wat is de General Data Protection Regulation?

1

Het beschermen van persoonlijke gegevens is een wettelijke verplichting, maar indien je als bedrijf actief bent in meerdere Europese lidstaten, ben je gebonden aan meerdere wetgevingen die soms van elkaar verschillen. Ook de manier waarop je met persoonlijke data omging en hoe je deze beveiligde was niet gespecifieerd. De GDPR verplicht je om na te denken over deze zaken.

Voor veel bedrijven staat er een rode cirkel op de datum van 25 mei 2018, de dag waarop de nieuwe GDPR van kracht wordt. Over deze verordening zijn er nog veel vraagtekens bij bedrijven, maar ook is het mij opgevallen door mijn onderzoek dat GDPR nog te weinig aandacht kreeg onder de data subjects zelf. Mijn doel in dit hoofdstuk is dan ook om GDPR te kaderen wat deze nieuwe verordening is en waarom deze verordening er komt.

[1] Cartoon: *https://marketoonist.com/2017/10/gdpr.html*

3.1 Regelmatig terugkerend vakjargon

GDPR maakt veelvoudig gebruik van vakjargon, deze staat hierboven in de verklaren woordenlijst. De meest gebruikte som ik hier nog even op.

(Data) Controller: Dit is de verwerkingsverantwoordelijke, de organisatie of persoon die het verwerkingsdoel van persoonlijke gegevens opstelt en bepaalt hoe deze gegevens verwerkt moeten worden.

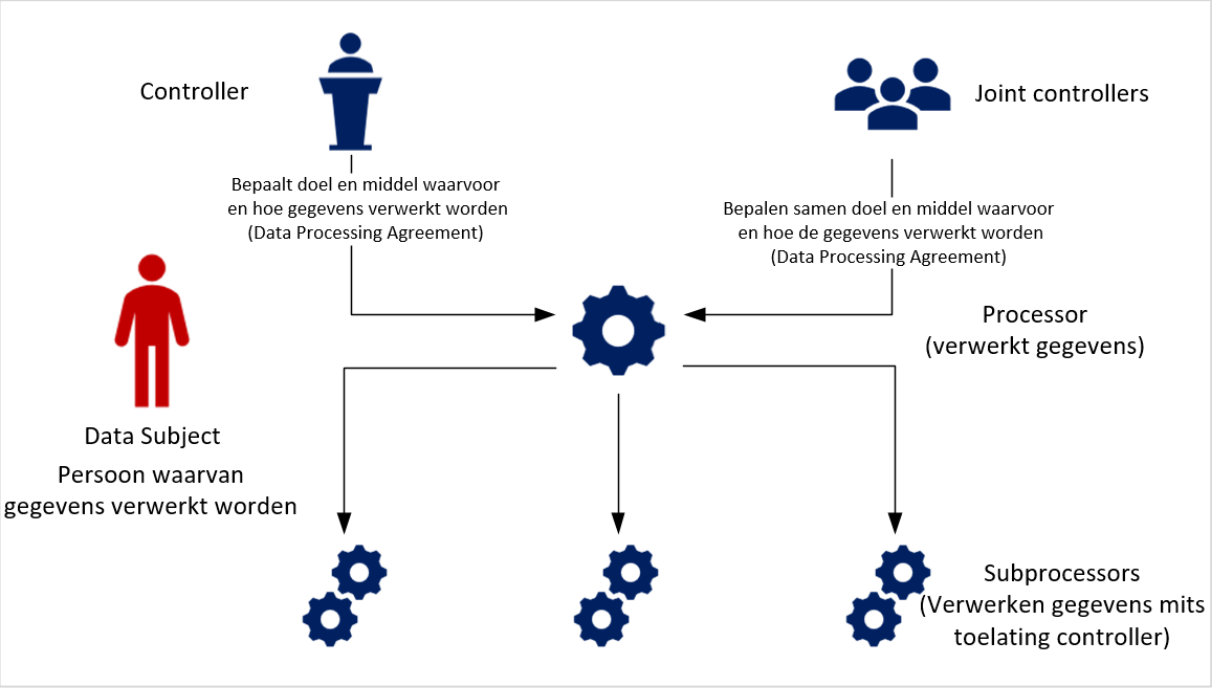
Joint (data) controllers: Dit zijn 2 controllers die samen een verwerkingsdoel bepalen en samen de middelen beslissen over hoe deze verwerking met betrekking tot persoonsgegevens zal gebeuren.

(Data) Processor: Dit is de verwerker, die handelt in opdracht van de controller.

Data-subject: Dit is de betrokken persoon van wie de persoonsgegevens zijn.

Persoonsgegevens: Gegevens van geïdentificeerde of identificeerbare natuurlijke persoon.

Sub processors: Processors die onder een processor verwerkingen uitvoeren mits de toelating of het informeren van de controllers.



3.2 Het kader van de GDPR?

Voor de GDPR bestond, had elke Europese lidstaat zijn eigen wetgeving omtrent bescherming van persoonsgegevens van Europese burgers en hun privacy en veiligheid. Maar de oude wetgeving werd achterhaald, dit omdat organisaties de behoefte kregen om online gedrag te analyseren en erop in te kunnen spelen.

Door de weinig duidelijke richtlijnen begonnen deze organisaties enorme hoeveelheden data te verzamelen zonder duidelijk hiervoor de betrokken persoon te informeren of toestemming te vragen. Daarnaast had de gebruiker van het systeem meestal geen vrije keuze, waardoor hij om de dienst te kunnen gebruiken verplicht werd om zijn of haar gegevens vrij te geven voor verdere verwerkingen.

Als gevolg van deze problematiek werd de GDPR op 14 april 2016 goedgekeurd door het Europese Parlement. Omwille van de grote impact werd beslist dat de verordening pas effectief van kracht zou gaan vanaf 25 mei 2018.

Merk op dat de GDPR een algemene Europese verordening is, die aangevuld kan worden door nationale bepalingen, andere nationale (uitvoerings-)wetgevingen maar ook door andere verordeningen zoals de E-Privacy verordening die er binnenkort zal aankomen.

3.3 De grote toevoegingen aan de GDPR

In tegenstelling tot wat velen denken is de GDPR niet een volledig nieuwe wetgeving. De GDPR is grotendeels een samenstelling uit oude gegevensbeschermingswetgevingen van verschillende lidstaten die nu samengevoegd wordt onder de GDPR-wetgeving. Toch zijn er enkele belangrijke verschillen.

1. **Security & Privacy by design:**
   De GDPR schrijft voor dat vanaf het begin van de ontwikkeling, rekening gehouden moet worden met beveiliging van gegevens en de privacy van de gebruikers.
2. **Dataretentie periodes:**
   Een probleem voor de GDPR was dat data die verzameld werd geen bewaartermijn had. Veelal werden persoonsgegevens oneindig bewaard. De GDPR pakt dit probleem aan door bedrijven te verplichten een bewaartermijn op hun gegevens te plaatsen in hun register van verwerkingsactiviteiten.
3. **Natuurlijke personen krijgen meer rechten:**
   De GDPR voorziet heel wat nieuwe rechten voor betrokken personen. Zoals het recht op **inzage**, het recht op **verbetering** of het recht om **vergeten** te worden. In het hoofdstuk "Welke impact heeft de GDPR op u en mij als data subjects?" bespreek ik de rechten die verworven zullen worden in meer details.
4. **Aanstelling Data Protection Officer:**
   Bij ondernemingen waar sprake is van systematische en/of grootschalige verwerking van persoonsgegevens is het aanstellen van een Data Protection Officer (Functionaris voor Gegevensbescherming in het Nederlands) verplicht. Deze functie zorgt ervoor dat het bedrijf conform blijft aan de GDPR door dat deze functie een **adviserende, informerende en controlerende rol** heeft omtrent IT-security en gegevensbescherming**.**
5. **Boetes voor niet naleven van de GDPR:**
   De GDPR heeft zware boetes voorzien voor degenen die de wet niet naleven. Deze kunnen variëren van 10 miljoen EUR of 2% van de globale jaar omzet of zelfs tot 20 miljoen euro of 4% van de globale jaar omzet (hoogste bedrag telt).
6. **Meer bijzondere categorieën van persoonsgegevens:**
   De GDPR beschouwt nu meer gegevens als persoonsgegevens waarbij een uiterst voorzichtige aanpak moet gehanteerd worden bij de verwerking ervan. Voorbeelden zijn ras of etnische afkomst, politieke opvattingen, religieuze overtuigingen, … genetische gegevens, biometrische gegevens, gegevens in verband met seksuele geaardheid, ….
7. **Recht op data portabiliteit:**

De nieuwe verordening voorziet ook in een nieuw recht voor betrokken personen. Namelijk het recht om data over te dragen naar een concurrent van de verwerkingsverantwoordelijke. Dit recht wordt verder uitgelegd in het hoofdstuk: “Welke impact heeft de GDPR op u en mij als data subjects?”.

3.4 Doelen van de GDPR

Het hoofddoel van GDPR is de bescherming van de Europese burger, dit door meer controle te geven aan de betrokken personen over de manier waarop hun gegevens verwerkt worden.

Maar verder is het ook **een uniform wetgevend kader** die wordt aangeboden. Dit kader is van kracht in alle lidstaten van de Europese Unie. Dit om de administratie en naleving van de wet te vereenvoudigen voor bedrijven die in meerdere Europese landen actief zijn. Aangezien er een Europese verordening is, kan **de rechtspraak beter op elkaar afgestemd** worden.

3.5 De scope van de GDPR, wanneer ben je nu precies onderworpen?

Je bent onderworpen aan de GDPR als je voldoet aan één van deze twee voorwaarden:

- Je bent **een organisatie met een vestiging binnen de Europese Unie**. Een vestiging kan hierbij ruim geïnterpreteerd worden: in sommige gevallen is het hebben van 1 persoon die werkt met persoonsgegevens hier al voldoende om als vestiging beschouwd te worden.
- Indien je geen Europese vestiging hebt maar wel **duidelijk diensten of goederen probeert aan te bieden gericht aan data subjects van de Europese Unie**. (Bv. door het aanbieden van wereldwijde verzending).

4 Welke impact heeft de GDPR op u en mij als data subjects?

GDPR zal voor verschillende partijen nieuwe rechten en plichten betekenen, maar wat betekent dit concreet voor u en mij, de natuurlijke personen, of data subjects in dit verhaal? In dit stuk komt u te weten welke nieuwe rechten u zal verkrijgen vanaf 25/05/2018.

Elke data subject verkrijgt:

1. *Recht van inzage van de betrokkene*
2. *Recht op rectificatie*
3. *Recht op beperking van de verwerking*
4. *Recht op verzet tegen een geautomatiseerde beslissing*
5. *Recht op wissing*
6. *Kennisgevingsplicht uitvoering rechten van een betrokkene*
7. *Recht op overdracht*
8. *Recht op bezwaar*
9. *Recht op notificatie na een inbreuk*

Hieronder een extra woordje uitleg om concreet uw rechten duidelijk te maken.

4.1 Recht van inzage van de betrokkene

Een betrokken persoon mag aan de controller (verwerkingsverantwoordelijke) navraag doen of zijn persoonlijke data effectief verwerkt wordt of niet. Indien persoonlijke data effectief verwerkt wordt mag de betrokken persoon die data inzien en moet de controller de persoon in kwestie ook meedelen welke rechten hij of zij heeft met betrekking tot die data en hoe hij of zij die rechten kan uitoefenen.

De verwerkingsverantwoordelijke heeft hier initieel 30 dagen de tijd voor maar kan deze termijn 2 maal met 30 dagen verlengen.

De verwerkingsverantwoordelijke moet u dus uiterlijk binnen 90 dagen het volgende meedelen:

- wat het doel of de reden is waarom uw persoonsgegevens verwerkt worden,
- welke categorieën van uw data verwerkt worden (Zie Bijlage 1: Categorieën van persoonsgegevens),
- met welke andere partijen uw gegevens gedeeld worden,
- hoelang uw gegevens bewaard zullen worden,
- dat u het recht heeft om een klacht neer te leggen bij de Gegevensbeschermingsauthoriteit (GBA),
- de oorsprong of de bron van de verzamelde gegevens over u,
- het eventueel bestaan van geautomatiseerde besluitvorming, profilering en het belang en de verwachte gevolgen dat deze beslissingen zullen hebben van deze verwerking op u,
- welke waarborgen er genomen zijn om uw persoonlijke gegevens te beschermen indien deze gedeeld worden met derde partijen.

Ook heeft u het recht op een gratis kopie van de persoonsgegevens die over u verzameld en/of verwerkt worden. Indien u bijkomende kopieën vraagt kan de controller wel een vergoeding vragen die gelijkstaat aan de gemaakte administratieve kosten.

Case Facebook

Tot voor kort was Facebook zeer onduidelijk welke data ze over gebruikers verzamelden, dankzij de GDPR is dit ietwat verbeterd. Het recht van inzage kan ruim worden geïnterpreteerd, dit wil niet enkel zeggen dat gebruikers van Facebook recht hebben om een kopie te krijgen van hun gegevens. Ze moeten ook inzage geven waar gebruikers hun rechten kunnen uitvoeren.

Uw rechten uitoefenen op Facebook kan trouwens via volgende link:

www.facebook.com/settings?tab=your_facebook_information.

Verder valt onder dit recht ook dat alle gebruikers het recht hebben om inzage te krijgen hoe hun data verzameld wordt maar ook hoe deze gebruikt zal worden. Facebook heeft recent hun Data Policy bijgewerkt om dit overzichtelijker te maken naar hun gebruikers.

Dit overzicht kan u vinden als u volgende link volgt:

www.facebook.com/privacy/explanation.

4.2 Recht op rectificatie

Dit recht biedt de mogelijkheid om foutieve of onvolledige gegevens aan te vullen of te verbeteren. Natuurlijk rekening houdende met het doel van de gegevensverwerking.

Case Examen

Het invullen van examens telt ook als persoonsgegevens, ook de antwoorden. Door de context van de gegevens kan het recht op verbetering niet gebruikt worden voor de aanpassing van de antwoorden van het examen. Maar de persoon kan wel zijn recht gebruiken om zijn foutief geschreven naam te corrigeren.

4.3 Recht op beperking van de verwerking

In sommige gevallen wilt u niet dat de controller uw persoonlijke gegevens wist. In dat geval kunt u zich beroepen op het recht op beperking van verwerking. Als u zich hierop beroept moet de controller zonder onnodige vertraging de verwerking beperken.

Je kan je beroepen op dit recht indien:

- je betwist dat je persoonlijke gegevens niet nauwkeurig zijn. Door dit recht in te roepen wordt de verwerking gestopt zolang nodig is om deze nauwkeurigheid te controleren,
- de verwerking van persoonsgegevens onrechtmatig is en u wilt niet langer dat uw data op dergelijke manier verwerkt wordt. (Bv. wanneer er onnodige data gevraagd wordt voor de doelverwerking),
- wanneer de data zal gewist worden omdat deze niet langer nodig is maar u niet wilt dat deze zal verwijderd worden omdat u dit nodig hebt om een gerechtelijke claim uit te voeren,
- je je wil verzetten tegen verwerking van de gegevens.

Case bankieren

Bank X brengt een nieuwe lening op de markt die zeer voordelig is bij het aangaan van een hypothecaire lening.

Een klant van bank Y merkt deze voordelige aanbieding op in een krantenartikel. En besluit om een hypotheek aan te gaan voor de aankoop van een vastgoed. Omdat hij echter uit gebruiksgemak alles wil centraliseren bij een bancaire instelling beslist hij om alle rekeningen en zijn andere bancaire producten over te dragen naar bank X.

Door deze beslissing vraagt de klant aan bank Y om al zijn persoonsgegevens te wissen.

Bank Y weigert dit echter omdat ze wettelijk verplicht zijn om alle gegevens 10 jaar bij te houden.

Hierop roept de klant zijn recht op beperking in. Dit zorgt ervoor dat de gegevens die wettelijk bewaard moeten worden door bank Y voor geen enkel ander doeleinde of verwerking mogen gebruikt worden.

4.4 Recht op verzet tegen een geautomatiseerde beslissing

U als data subject heeft het recht om u te verzetten om onderworpen te worden tegen geautomatiseerde verwerking of profilering waaraan voor u rechtsgevolgen of directe gevolgen aan gekoppeld zijn, (bv. zoals geweigerd worden voor een sollicitatiegesprek, doelgerichte en individuele reclameaanbiedingen in supermarkten, …).

Enkel in volgende gevallen is geautomatiseerde besluitvorming waaronder profilering toegestaan:

- het proces is nodig voor de afsluiting of uitvoering van een overeenkomst tussen de betrokkene en controller,
- het wettelijk toegestaan is door de wetgeving,
- de betrokkene of data subject zijn uitdrukkelijke toestemming gaf.

Case Target Corporation

Elke keer als je gaat winkelen en je maakt gebruik van je klantenkaart, geef je zonder dit te beseffen je consumptiegewoontes prijs. Op zich niets verkeerd mee. Toch?

Wel Target, een Amerikaanse supermarkt-keten begon op al die persoonsgegevens data mining toe te passen om statistische conclusies te trekken. Door klanten te gaan groeperen volgens de producten die ze kochten konden ze, onder andere, zwangere vrouwen onderscheiden. Het is zelfs zo dat ze erin slaagden om met een kleine foutenmarge de uitgerekende datum van de bevalling te schatten.

Dit systeem werd gebruikt om reclamecoupons te sturen naargelang de dag van de bevalling naderde van mogelijks zwangere vrouwen. Nu is het zo dat dit deze reclame werd gestuurd naar een meisje van de middelbare school voor ze zelf wist dat ze zwanger was.

Dit is overduidelijk een voorbeeld waar, indien deze vorm van profilering toegepast zou worden binnen de Europese grenzen er sprake is van een overtreding van de GDPR-verordening.

4.5 Recht op wissing

2

Wellicht het meest besproken verworven recht in de GDPR-verordening, beter bekend als “the right to be forgotten”. U als betrokkene kan de controller verplichten uw persoonlijke data te laten verwijderen zonder onnodige vertraging. Merk op dat dit recht geen absoluut recht is en per casus moet afgewogen worden tegenover de belangen van verwerkingsverantwoordelijke. Dit recht kan ingeroepen worden indien er sprake is van onderstaande stellingen.

- De gegevens die verzameld werden niet langer nodig zijn voor de doeleinden waarvoor zij origineel verzameld of verwerkt werden. Dit recht is ook een plicht voor de controller aangezien het hier gaat over data minimalisatie en retentieperiodes die toegepast moeten worden.
- U trekt uw toestemming voor de verwerking van uw persoonlijke gegevens in, en er is geen andere rechtsgrond om de data te behouden.
- Indien uw gegevens onrechtmatig verwerkt worden.
- De persoonsgegevens moeten worden gewist in verband met een wettelijke verplichting.
- Indien er onrechtmatig persoonsgegevens verwerkt worden van kinderen.

[2] Cartoon: *https://www.slideshare.net/SagittariusMarketing/travelodge-gdpr-case-study*

Case Google – Right to be forgotten

Er zijn reeds 2 cases waarbij 2 zakenmannen zich hebben proberen beroepen op het “right to be forgotten”, dit nog voor de GDPR in voege was.

De eerste persoon was veroordeeld voor financiële fraude kreeg hiervoor een gevangenisstraf van 4 jaar. Door zijn veroordeling werd bij elke Google zoekopdracht op zijn naam de krantenartikels over zijn veroordeling weergegeven. Dit was een persoon met enige bekendheid in het publieke leven. Daarom vroeg hij aan Google om deze links te verwijderen. Google weigerde echter. De uitspraak was dat Google zich niet kon beroepen op basis van journalistieke vrijheid, echter door dat de persoon een publieke functie had en de veroordeling niet valt onder het privéleven deze aanvraag geweigerd werd.

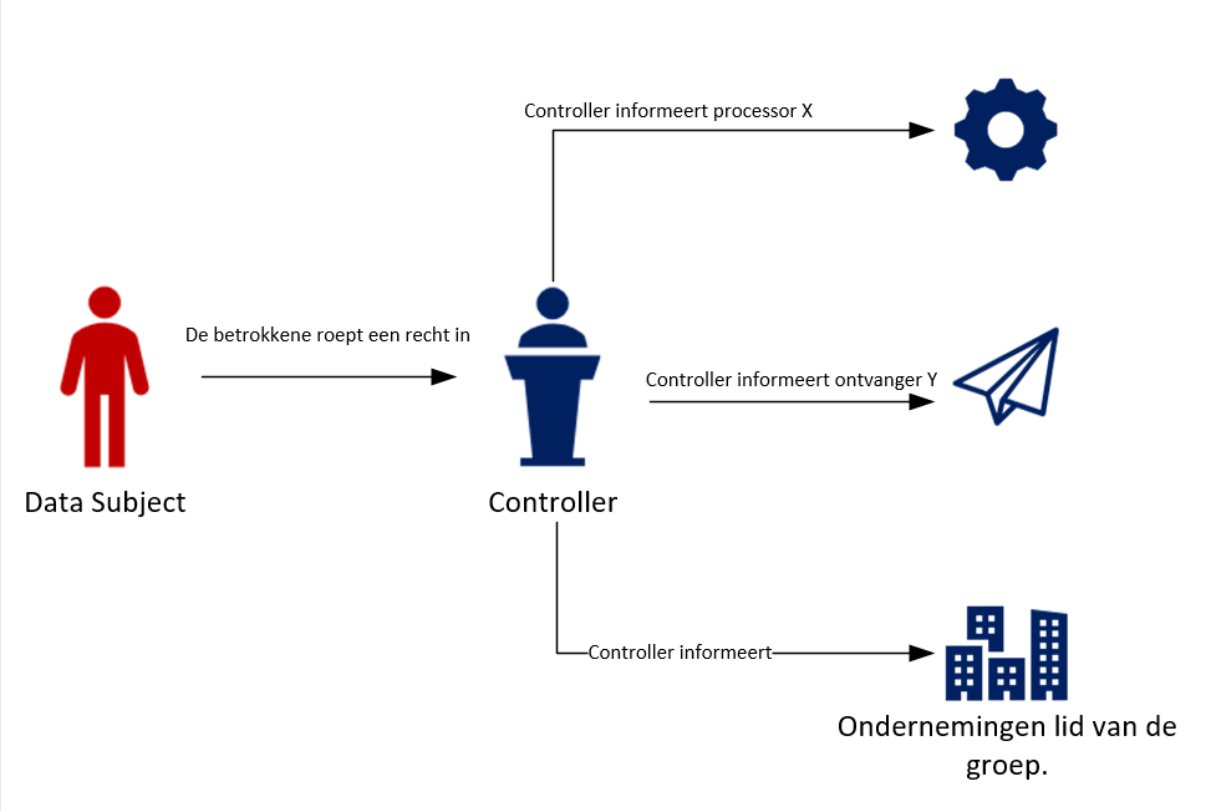
Een tweede zakenman die 10 jaar celstraf kreeg voor samenzwering en het onderscheppen van communicatie wou na zijn vrijlating zijn naam zuiveren van de zoekmachine Google. Google ging hier niet mee akkoord maar het Europees Gerechtshof zag dit anders. De uiteindelijke uitspraak in 2014 (voor GDPR bestond) was dat “irrelevante” en verouderde gegevens moesten gewist worden op aanvraag.

4.6 Kennisgevingsplicht uitvoering rechten van een betrokkene

Dit verworven recht is een plicht die opgelegd wordt aan de verwerkingsverantwoordelijke. Als je als betrokken persoon een van je andere rechten uitoefent, dan moet de verwerkingsverantwoordelijke alle andere partijen waarmee hij samenwerkt kennisgeven dat een betrokken persoon een van zijn rechten heeft ingeroepen.

Het gevolg is dat alle betrokken partijen dan ook hetzelfde recht moeten invullen zodat de betrokken persoon dit niet zelf voor elke partij moet doen.

De verwerkingsverantwoordelijke moet ook informatie kunnen verstrekken indien je vragen hebt over de ontvangers van je persoonsgegevens.



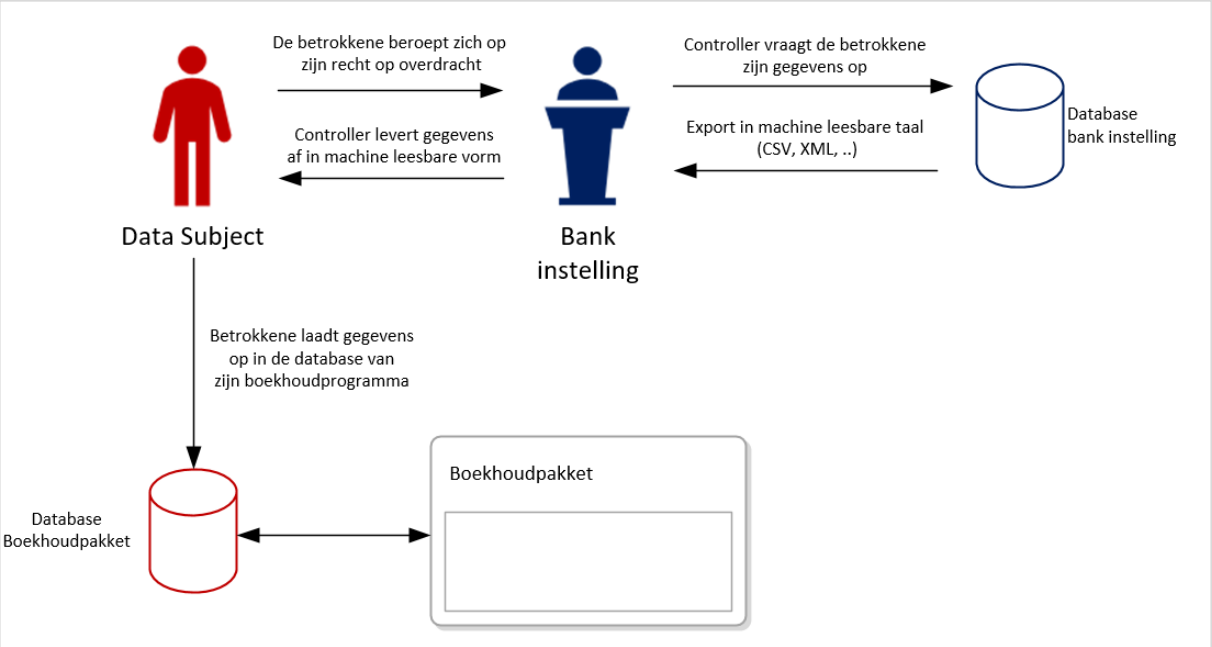
4.7 Recht op overdracht

Een betrokken persoon heeft ook het recht om zijn gegevens over te maken aan een andere verwerkingsverantwoordelijke. Daarom kan de betrokken persoon hier om een bijzondere kopie vragen in een gestandaardiseerd, machine leesbaar formaat. Voorbeelden hiervan zijn Comma Separated Value (CSV) bestanden, een kopie in JSON-formaat of een XML-bestand. Echter zijn er geen duidelijke afspraken over wat nu precies een gestandaardiseerd formaat is. Maar het is wel de bedoeling dat de andere verwerkingsverantwoordelijke het bestand kan gebruiken indien de betrokken persoon zich op dit recht wil beroepen.

Het is ook hier belangrijk om bij dit recht te vertellen dat het geen absoluut recht is. Het moet op zijn beurt afgewogen worden tegenover de rechten die de verwerkingsverantwoordelijke heeft. Een voorbeeld hiervan kan zijn het beschermen van intellectuele eigendom.

Ook kan dit recht pas ingeroepen worden in bepaalde gevallen. Hieronder staan ze opgesomd.

- De verwerking moet gebeuren onder de rechtsgrond (expliciete) “toestemming” of “contractuele noodzaak”.
- Bovenop een van geldige rechtsgronden moet de verwerking uitgevoerd worden door automatische middelen.



Een belangrijke noot van dit recht is dat dit gaat over gegevens die je zelf kenbaar hebt gemaakt. Een verwerkingsverantwoordelijke kan ook dit recht afwegen om de mogelijke resultaten van de verwerking niet kenbaar te maken. Dit kan bijvoorbeeld om het recht op bescherming van intellectuele eigendom (zelf ontworpen algoritmes, ..) in te roepen.

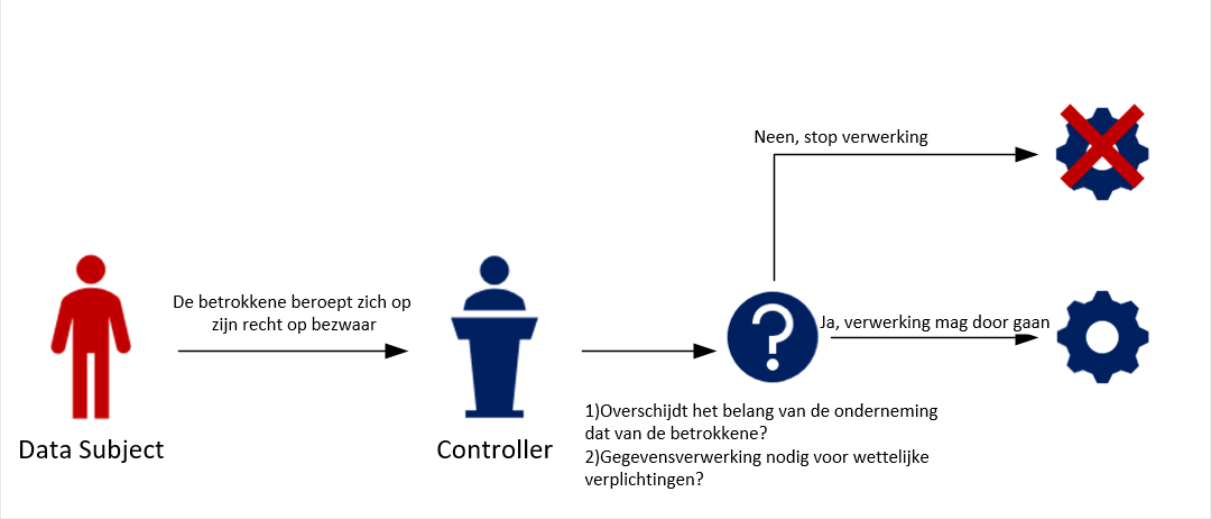
4.8 Recht op bezwaar

Indien een controller uw persoonlijke gegevens verwerkt op de grond van algemeen belang of legitiem belang mag u als data subject bezwaar aantekenen tegen verdere verwerking van deze gegevens.

Dit wil zeggen dat de controller het verwerken moet stopzetten tenzij:

- De controller kan aantonen dat er juridische grond is die het individueel belang overschrijdt.
- De controller de verwerking of de gegevens nodig heeft om zijn wettelijke rechten uit te oefenen en of te verdedigen.

Ook hebt u als data subject het recht om u te verzetten tegen gegevensverwerking indien het doel van verwerking direct marketing is. Hetzelfde geldt ook indien het gaat over wetenschappelijke, historische of statistische doeleinden tenzij de verwerking van algemeen belang is.



Dankzij mijn stage kon ik contacten leggen met heel wat nieuwe mensen. Via een van deze personen werd ik in contact gebracht met Michel Flamme, juridisch adviseur van de VRT. Ik heb hem enkele vragen gesteld over de impact van de GDPR op het uitvoeren van een functie binnen journalistiek en het maken van tv-programma's. Hieronder een schets van de problematiek die de GDPR volgens Michel zou kunnen hebben indien er geen uitzondering gemaakt zou worden voor de journalistiek.

Case journalistiek

De GDPR en het recht op journalistieke en artistieke vrijheid staan lijnrecht tegen over elkaar. Artikel 85 van de GDPR die spreekt over de verwerking en vrijheid van meningsuiting en van informatie, stelt dat er een uitzondering gemaakt moet worden voor deze specifieke doelverwerking. Journalistiek is een deontologisch beroep met de plicht om correct nieuws te verspreiden. Daarom is het van uiterst belang dat in de kaderwet die nu gestemd moet worden in het parlement een flexibele vrijheid is voor het uitoefenen van dit beroep.

Stel je immers voor dat zomaar iedereen recht op bezwaar, beperking of op vergetelheid kan inroepen. Dit zou kunnen leiden tot schending van de democratie, dit zou kunnen wanneer politici hun publieke uitspraken en fouten willen. Of erger, stel dat Marc Dutroux al zijn gegevens wil wissen, inclusief reportages, krantenartikels, archieven, … Dit voelt gewoon niet correct aan.

De verschillende persgroepen hebben dan ook een aangepast wetsvoorstel gedaan voor de bescherming van journalistiek. Dit omdat het huidige voorstel zeer beperkt was. Het aangepast voorstel moet de pers meer flexibiliteit bieden voor het uitoefenen van hun beroep.

Ook de artistieke vrijheid werd meegenomen in dit nieuwe voorstel. Want stel dat programmamakers plots alle opnames moeten verwijderen die uitgezonden zijn omdat iemand een recht onder de GDPR inroept. Het is niet de schuld van de pers als je in een bepaald programma een negatief imago zou krijgen. Vandaar dat de artistieke vrijheid ook moet beschermd worden.

4.9 Recht op notificatie na een inbreuk

Wanneer er een inbreuk is in verband met persoonsgegevens die een hoog risico inhouden voor de betrokken personen hebben die het recht hierop van op de hoogte gebracht te worden.

Deze melding moet in klare, duidelijk en voor iedere betrokken persoon in een begrijpbare taal gebeuren. Dus niet in een juridisch formaat. De verwerkingsverantwoordelijke moet de melding brengen ten laatste 72u na dat deze zelf op de hoogte was van de inbreuk.

In de melding van de verantwoordelijke moeten volgende elementen aanwezig zijn om duidelijk te maken wat er precies gebeurd is, wat de mogelijke gevolgen zijn en waar contact kan opgenomen worden bij verdere vragen:

- De aard van de inbreuk (moedwillig, persoonlijke fout, enzovoorts).
- De contactgegevens van de Data Protection Officer, deze persoon is het contactpunt bij verdere vragen na een inbreuk.
- De mogelijke gevolgen van de inbreuk op de betrokken personen.
- Welke maatregelen de verantwoordelijke reeds genomen heeft om de inbreuk en de gevolgen ervan te beperken.

Indien de inbreuk effecten heeft op grote schaal, en de melding naar individuele personen te veel tijd of andere middelen kost, kan de melding vervangen worden door een publiek statement te maken die in een even efficiënte manier de betrokken personen bereikt.

Case Yahoo

In 2014 werd Yahoo gehackt en werden de gegevens van 500 miljoen gebruikers gestolen. Deze gegevens bevatten de namen, email adressen, telefoonnummers, geboortedatums, geëncrypteerde passwoorden en in sommige gevallen zelfs de security vragen die gebruikt worden in het geval een persoon zijn passwoord vergeet.

Vanwege het feit dat Yahoo, liever Altaba Inc. het bedrijf dat overbleef na de overname van Verizon Communications, deze inbreuk niet op tijd gemeld heeft werd hen door de US Securities and Exchange Commission een boete van 35 miljoen Amerikaanse Dollar opgelegd.

Altaba Inc. ging akkoord om de boete te betalen omdat ze de investeerders niet hebben geïnformeerd over de hacking tot 2 jaar na de feiten, in september 2016.

Yahoo maakte uiteindelijk in juli 2016 de inbreuk bekend naar het grote publiek, na de overname van Verizon. Verizon kocht echter hierdoor Yahoo niet volledig over en liet het stuk die verantwoordelijk was voor deze inbreuk achter.

5 Welke plichten heeft een data controller?

Voor de GDPR deden veel bedrijven aan intensieve data verzameling, want hoe meer je weet over je klanten of je doelpubliek, hoe makkelijker je de bedrijfsstrategie, missie, kan aanpassen om het bedrijf beter te gaan profileren op de markt om te gaan richten op deze specifieke groepen. Maar nu…

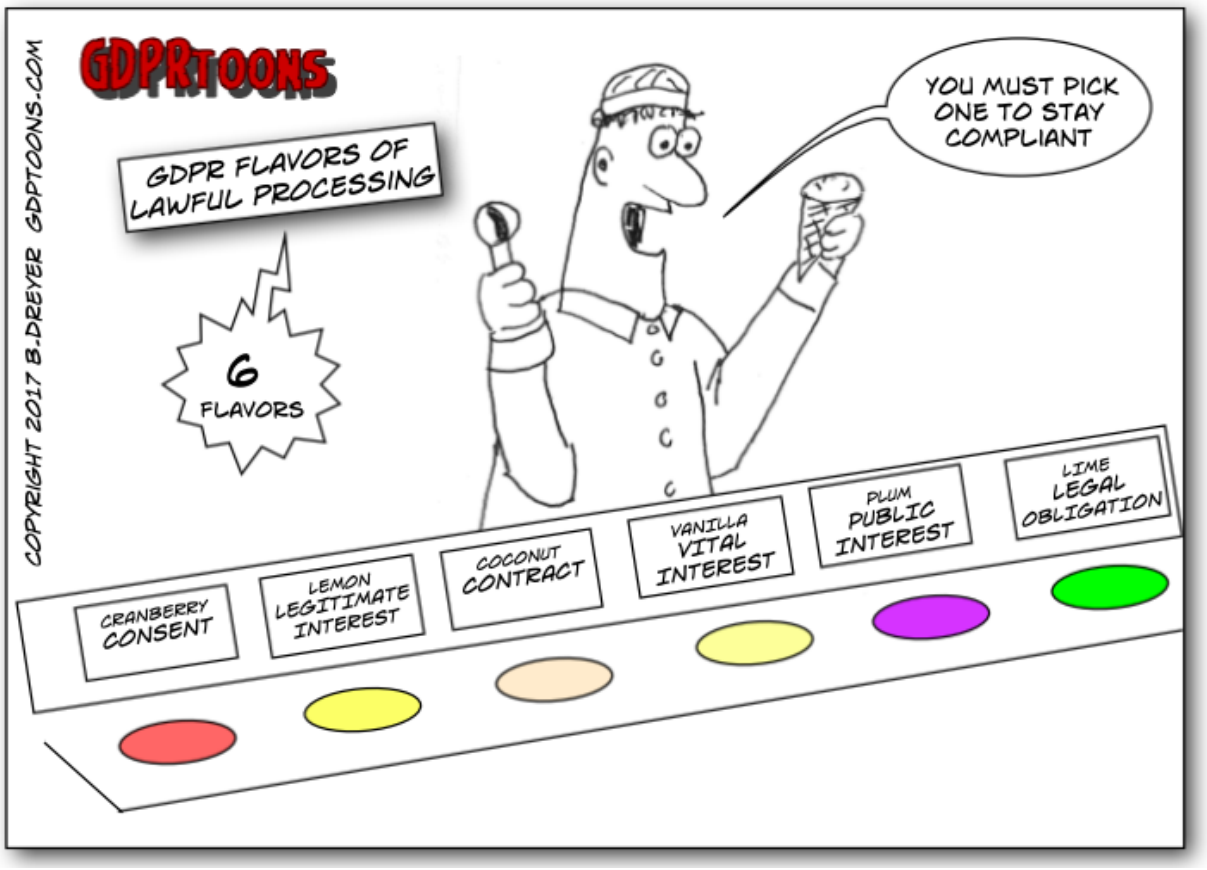
5.1 Hoe horen persoonsgegevens verwerkt te worden?

De GDPR heeft duidelijke regels wanneer en hoe je met persoonlijke data moet omspringen.

De verwerking van persoonsgegevens moet:

- op een **rechtmatige manier** gebeuren (Zie Op welke juridische grond mogen persoonsgegevens verwerkt worden?),
- op een **behoorlijke wijze** gebeuren,
- op een **transparant**e manier gebeuren,
- voor een **welbepaald, duidelijk gecommuniceerd doel** zijn; **zonder** deze data voor een ander dan het origineel bepaalde doel te gebruiken (**repurposing**),
- moet in evenwicht zijn met de persoonsdata die gebruikt wordt; je mag niet meer data verwerken dan nodig is voor het in ogen gestelde doel van verwerking (**data minimalization**),
- **juist zijn** wat wil zeggen dat deze indien nodig moeten worden geactualiseerd. Er moet op een redelijke manier gehandeld worden zodat deze foutieve data gewist of gecorrigeerd kan worden,
- indien deze voor andere doelen verwerkt (zullen) worden, op een manier gebeuren dat de betrokkene (data subject) **niet** langer kan **geïdentificeerd** kan worden,
- gebeuren **met security en privacy by default of by design** in het achterhoofd (Zie Welke impact heeft GDPR op IT Security?),
- de data controller of verwerkingsverantwoordelijke moet alle bovenstaande punten kunnen **aantonen en bewijzen**.

5.2 Op welke juridische grond mogen persoonsgegevens verwerkt worden?



3

GDPR stelt dat voor elke verwerking van persoonsgegevens een juridische grond moet zijn om deze te mogen verwerken. Er zijn 6 mogelijkheden:

1. **De betrokken persoon of data subject geeft toestemming voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.**

   Indien de juridische grond toestemming ('consent') is, dan moet er toestemming voor elk apart verwerkingsdoel gevraagd worden. Ook moet het data subject op een actieve manier zijn toestemming geven, impliciete toestemming (een passieve handeling zoals verder surfen op een website) is dus geen geldige grond voor verwerking. De betrokken persoon moet ook op een even makkelijke manier zijn toestemming kunnen terugtrekken als die gegeven is.

Case Cookies

[3] Cartoon: *http://www.gdprtoons.com/2017/08/the-gdpr-provides-six-6-grounds-for_29.html*

Op het moment van schrijven is er wat onduidelijkheid over cookie consent in de GDPR, grotendeels omdat de nieuwe E-privacy verordening is uitgesteld. Een ding is wel duidelijk, consent of toestemming moet even makkelijk teruggetrokken kunnen worden als die gegeven is.

Maar het is wel zo dat er geen toestemming moet gevraagd worden voor functionele cookies. Dit zijn de cookies die noodzakelijk zijn voor de goede werking van de website zoals voor het voorzien van login functionaliteit.

Een ander probleem is dat ook analytische cookies en meer bepaald Google Analytics door veel bedrijven als een noodzakelijke cookie gezien worden. Dit is incorrect en voor dit soort cookies moet er dus wel degelijk toestemming worden gevraagd.

De conclusie is dat er weinig tot geen ingebouwde mogelijkheid voorzien om de gegeven toestemming voor cookies opnieuw in te trekken. Er wordt vaak verwezen naar de gebruikte internetbrowser om je cookies te verwijderen. Deze manier is duidelijk niet even simpel als het klikken op een cookiebanner dat je akkoord gaat. Dit is dus geen goede methode volgens de GDPR.

Een ander voorbeeld meer gericht naar Google Analytics dat ik gezien heb in een privacy statement, is een verwijzing naar een pagina van Google. Op deze pagina kan een add-on gevonden worden om te installeren (https://tools.google.com/dlpage/gaoptout) indien je niet akkoord gaat met het gebruik van Google Analytics.

Dit gaat nog een stap verder want hier moet je al iets installeren om niet akkoord te gaan met het gebruik van Google Analytics en werd in de eerste instantie je toestemming voor het gebruik van Google Analytics niet expliciet gevraagd. Ook deze methode is dus niet voldoende volgens de GDPR.

2. **De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene voor de sluiting van een overeenkomst maatregelen te nemen.**

   Als de juridische grond een contract of overeenkomst is, dan is er een nadruk op de noodzakelijkheid. Een voorbeeld om dit te verduidelijken:

   Kinepolis heeft een onlineverkoopdienst waarbij klanten tickets kunnen kopen om naar de film te gaan. Bij de online aankoop van een ticket worden de voornaam, naam en het e-mailadres gevraagd. Deze gegevens zijn nodig voor de verwerking aangezien je een gepersonaliseerde e-mail zal krijgen met daarin je tickets die je hebt aangekocht. Tickets aangekocht op het internet staan namelijk op naam. Er wordt ook een geslacht gevraagd, dit is in het gerechtvaardigd belang om de mails op een klantvriendelijke manier te versturen. Een online verkoop heeft dus minimaal deze gegevens nodig om de verkoopovereenkomst af te kunnen sluiten.

   Indien in bovenstaand voorbeeld ook het adres zou gevraagd worden, zou dit ongegrond zijn aangezien deze informatie niet nodig is voor de uitvoering van de overeenkomst.

3. **De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.**

Onder deze verwerkingsgrond vallen alle wettelijke verplichtingen die de controller moet uitvoeren. Een voorbeeld zijn kastickets die een maand bijgehouden worden als bewijslast van schade, diefstal en/of fraude. Facturen moeten 2 jaar bijgehouden worden als bewijslast voor garanties.

4. **De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen.**

   De verwerking van persoonlijke gegevens is van levensnoodzakelijk belang. Zoals wanneer de betrokkene op de spoeddienst ligt en zijn bloedgroep moet geraadpleegd worden om een bloedtransfusie uit te voeren.

5. **De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.**

   De verwerking van de persoonsgegevens is in het belang van elke natuurlijk persoon, een voorbeeld hiervan is onderzoek dat gevoerd wordt naar kanker. Deze verwerking gebeurt in het kader van de volksgezondheid en mag daarom mits de nodige beschermingsmaatregelen doorgaan. De verwerking moet dan ook strikt beperkt blijven binnen dit bepaalde kader en er moeten bewaartermijnen worden toegekend en nageleefd worden.

6. **De verwerking is van gerechtvaardigd belang ten aanzien van de verwerkingsverantwoordelijke.**

   Hier is de verwerking geldig als de belangen of grondrechten en of fundamentele vrijheden van het betrokken individu niet overschreden worden ten opzichte van het gerechtvaardigd belang van de controller. Dit wil zeggen dat de verwerking in balans moet zijn met het data subject zijn rechten. Dit kan afgetoetst worden door het uitvoeren van een zogeheten “balancing test”. In zo’n test worden de belangen tussen de betrokken persoon en controller afgewogen.

   Als voorbeeld en om dit beter visueel te kunnen voorstellen is er een fictief voorbeeld te vinden onder Bijlage 5: Voorbeeld van een balancing test.

5.3 Op welke grond mogen persoonsgegevens van een bijzondere categorie verwerkt worden?

[4]

Strikt genomen is de verwerking van persoonsgegevens die vallen onder bijzondere categorieën onder GDPR verboden. Deze categorieën zijn gegevens omtrent:

- ras of etnische afkomst,
- religieuze of filosofische overtuiging,
- genetische data of biometrische data die gebruikt kan worden voor de identificatie van een natuurlijk persoon,
- gezondheid,
- het seksleven of seksuele voorkeur van een natuurlijk persoon.

Om deze verwerking toch geldig te maken onder GDPR zijn er toch enkele verwerkingsgronden:

- Wanneer de betrokkene **uitdrukkelijke toestemming** geeft voor een welbepaald doel. De verwerking moet dus duidelijk en transparant zijn zodat de betrokkene weet heeft wat er met deze data zal gebeuren.

- Wanneer de verwerking noodzakelijk is voor het **uitvoeren van verplichtingen en/of rechten van de controller of betrokkene**. Dit kan zijn voor de uitvoeringen van bijvoorbeeld het arbeidsrecht, sociale zekerheid, … De lokale nationale wetgevingen moeten nog steeds gevolgd worden zodat de grondrechten en fundamentele belangen van de betrokkene behouden worden.

[4] Cartoon: *https://actnowtraining.files.wordpress.com/2016/10/illust_01_e.jpg*

- De verwerking is noodzakelijk van **vitaal belang (levensbelang)** voor de betrokkene of van een andere natuurlijke persoon waarbij de betrokkene fysiek of juridisch niet in staat is om toestemming te geven. Bv wanneer de betrokkene op de spoeddienst van een ziekenhuis dringende medische zorg nodig heeft.

- De verwerking wordt verricht door bijvoorbeeld een vzw die op **politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is**. Dit zijn voor dit soort verenigen hun gerechtvaardigde verwerkingsactiviteiten. Maar om de verwerking gegrond te maken moeten er waarborgen gesteld worden die de gegevens van de betrokkene veiligstellen.

- De verwerking is noodzakelijk voor **preventieve- of arbeidsgeneeskunde**. Zoals bijvoorbeeld de beoordeling van arbeidsgeschiktheid en het verlenen van gezondheidszorg aan de betrokkene.

- De verwerking en/of archivering van persoonsgegevens is noodzakelijk voor het **algemeen belang** op gebied van **volksgezondheid**. Een voorbeeld hiervan is onderzoek naar kanker.

- De verwerking is noodzakelijk voor de **uitvoering of onderbouwing van een rechtsvordering**. Een voorbeeld kan hier zijn DNA gebruiken als bewijslast in een moordzaak.

Zoals je ziet staan de woorden “uitdrukkelijke toestemming” en “noodzakelijk” onderlijnd. Dit is omdat je moet kunnen aantonen dat de betrokkene deze toestemming heeft gegeven en/of dat de verwerking van de persoonsgegevens noodzakelijk is voor de doelverwerking gezien in het vet.

5.4 Het registreren van de verwerking van persoonsgegevens

Elke controller (verwerkingsverantwoordelijke) moet vanaf 25 mei een register van zijn verwerkingsactiviteiten kunnen voorleggen indien gevraagd door de Gegevensbeschermingsautoriteit (GBA). Het register moet wettelijk gezien minimum de volgende data bevatten (vanuit het standpunt van een controller):

- De naam en contactgegevens en eventuele joint-controllers en indien aanwezig, de vertegenwoordiger van de controller en de “Data Protection Officer”.
- Het doel van de verwerking van persoonsgegevens.
- De categorieën van verwerkte gegevens. (Zie Bijlage 1: Categorieën van persoonsgegevens)
- De categorieën van alle ontvangers of partijen aan wie de persoonsgegevens kenbaar zijn gemaakt of kenbaar gemaakt zullen worden. Dit betreft ook derden (andere landen en/of internationale organisaties, zie Bijlage 2: Categorieën van ontvangers).
- Indien de gegevens getransfereerd worden naar een ander land of internationale organisatie moeten deze opgenomen worden in het register.
- De retentieperiode van de gegevens, dit is de periode hoe lang de gegevens worden bijgehouden.
- Waar mogelijk en indien van toepassing een beschrijving welke technische of organisatorische maatregelen er genomen werden om de gegevensverwerking veilig te laten verlopen.

Zie Bijlage 4: Voorbeeld register van verwerkingsactiviteiten voor een ingevuld voorbeeld.

5.5 Meldingsplicht van inbreuken aan de Gegevensbeschermingsautoriteit

Indien er zich een inbreuk voordoet waarbij persoonlijke gegevens betrokken zijn, moet de controller zonder vertraging, binnen 72 uur na het ontdekken van de inbreuk, deze melden bij de Gegevensbeschermingsautoriteit. Tenzij deze inbreuk niet zal leiden tot een hoog risico op de rechten en vrijheden van de betrokken natuurlijke personen. Om het risico te bepalen moet de controller een risicoanalyse uitvoeren, maar er zal een kader geleverd worden door de Gegevensbeschermingsautoriteit om dit te verduidelijken.

Wanneer er een inbreuk plaats vond die gemeld moet worden aan de Gegevensbeschermingsautoriteit, dan moet deze melding duidelijk geformuleerd worden met volgende informatie:

- De omstandigheden van de inbreuk (hacking, diefstal, …), het aantal getroffen data subjects en de categorieën van de betrokken persoonlijke gegevens (Bijlage 1: Categorieën van persoonsgegevens) met het aantal records die betrokken waren bij de inbreuk.
- De naam en contactgegevens van de Data Protection Officer of het contactpunt waar verdere informatie kan gevraagd worden.
- Een beschrijving van de mogelijke gevolgen van de inbreuk
- Een beschrijving van de reeds genomen of geplande acties en maatregelen die genomen werden of zullen genomen worden om de inbreuk aan te pakken of om verdere consequenties te reduceren.

Deze gegevens kunnen, indien nodig, op verschillende tijdstippen geleverd worden aan de GBA, maar deze gegevens moeten zonder vertraging ingediend worden. Een voorbeeld kan zijn dat de controller afweet van een inbreuk maar op het moment van de melding niet meteen een zicht heeft op de gevolgen, dan moet de controller eerst een onderzoek uitvoeren en zo snel mogelijk deze informatie meedelen aan de Gegevensbeschermingsautoriteit.

Ook moet de controller elk incident of inbreuk bijhouden in een logbestand samen met de genomen maatregelen. Dit document kan opgevraagd worden door de GBA om te controleren of artikel 33 van de GDPR-wetgeving nageleefd wordt.

Voor een visuele voorstelling zie Bijlage 3: Schema rapporteren van inbreuken betreffende persoonsgegevens.

5.6 Meldingsplicht van inbreuken aan de data subject

Wanneer een inbreuk een mogelijk hoog risico inhoudt op de rechten en vrijheden van een betrokken persoon en wanneer er **geen maatregelen** genomen werden om de persoonsgegevens te beschermen moet de controller of verwerkingsverantwoordelijke de betrokken personen van de inbreuk zo snel mogelijk contacteren en informeren.

Hier zijn wel **uitzonderingen** aan verbonden. Zoals wanneer ervoor gezorgd werd dat de gegevens onherkenbaar gemaakt zijn. Om dit te bereiken kunnen verschillende manieren toegepast worden zoals:

- De betrokken gegevens zijn **onbegrijpelijk** door bv. het gebruik van sterke encryptie, rekening houdend met de technologie die op het moment beschikbaar is.
- Het **anonimiseren** van de gegevens: het verwijderen van elke mogelijke data die het mogelijk maakt om de betrokken persoon te identificeren
- Het **pseudonomiseren** van de gegevens: het verwijderen van de link tussen gegevens die het mogelijk maakt om de betrokken persoon te identificeren

- Het toepassen van een sterk IT-beleid (Zie De impact van GDPR op IT Governance & IT Security)

Pseudonomiseren kan bereikt worden door bijvoorbeeld de onderstaande 2 cases te implementeren.

- De naam te vervangen door een ID en de naam in een andere database op te slaan.
- Het gebruik van tokenization die persoonlijke data vervangt in de records.

Voor een visuele voorstelling zie Bijlage 3: Schema rapporteren van inbreuken betreffende persoonsgegevens.

5.7 Wat is een Data Protection Impact Assessment (DPIA)?

GDPR legt met ingang van 25/05/2018 de verantwoordelijkheid voor de verwerkingsprocessen bij de controller. Dit houdt in dat de controller dus maatregelen moet treffen om deze processen op een veilige manier uit te voeren. Daarnaast is GDPR ook een risico gebaseerde verordening, wat wil zeggen dat risico's moeten afgewogen worden door de verwerkingsverantwoordelijke.

Een Data Protection Impact Assessment is een **risicoanalyse** die helpt bij de controle of bedrijven de juiste veiligheid implementeren en of de rechten van betrokkenen beschermd worden. Het resultaat van zo'n test kan gebruikt worden om verbeteringen aan te brengen aan het verwerkingsproces en zo dus inbreuken betreffende persoonsgegevens te vermijden.

Deze analyse moet uitgevoerd worden wanneer gebruik gemaakt wordt van **nieuwe technologieën** en wanneer het verwerkingsproces een **hoog risico** inhoudt op de rechten van betrokken personen. Hieronder vallen de systematische en uitgebreide processen die een **rechtsgevolg** hebben, **grootschalige verwerking** van **speciale categorieën** van persoonsgegevens, grootschalige verwerking van gegevens die gaan over **veroordelingen** en strafbare feiten of waar op grote schaal openbaar **toegankelijke ruimtes gemonitord** worden zoals het gebruik van camerabewaking.

Deze analyse heeft geen vast sjabloon of 'template' die gebruikt kan worden maar heeft wel enkele wettelijk verplichte zaken die opgenomen moeten worden in het eindresultaat.

- Een beschrijving van het doel van verwerking, en indien legitiem belang de verwerkingsgrond is moet deze ook beschreven staan.
- Een controle of de verwerking noodzakelijk en proportioneel is.
- Een risicoanalyse.
- Getroffen maatregelen om de risico's van de verwerking te verlagen.

Zie "Bijlage 6: Voorbeeld van een DPIA" voor een ingevuld voorbeeld van een DPIA, gemaakt met de software van CNIL.

5.8 De "Data Protection Officer (DPO)"

GDPR brengt ook een nieuwe verantwoordelijkheid met zich mee. Namelijk die van de functionaris inzake gegevensbescherming, ook wel Data Protection Officer (DPO) genoemd. De DPO is de verantwoordelijke die de strategie voor de gegevensbescherming en de implementatie overziet. De DPO heeft een controlerende, informerende en adviserende rol. De DPO mag ook andere functies uitvoeren zolang dat dit niet resulteert in een belangenconflict.

Een groot misverstand van GDPR is dat iedereen een DPO nodig heeft, dit is zeker niet waar maar is slechts in drie welbepaalde gevallen verplicht. Merk wel op dat de Belgische Gegevensbeschermingsautoriteit het sterk aanraadt, zelfs indien het niet verplicht is, om toch een DPO aan te stellen.

- De verwerking van persoonsgegevens wordt uitgevoerd door een publieke autoriteit (bv. De Rijksdienst voor Sociale Zekerheid).
- Wanneer de verwerking, vanwege de aard, omvang of doeleinden op grote schaal gebeurd.
- Bij grootschalige verwerking van gegevens die vallen onder de bijzondere categorieën of bij gegevens in verband met strafrechtelijke veroordelingen of strafbare feiten.

De DPO heeft geen specifiek profiel maar moet wel de nodige kennis in verband met gegevensbescherming hebben om deze rol naar behoren uit te voeren.

Bij nieuwe of geplande wijzigingen aan een verwerkingsproces of alle andere mogelijke gelegenheden betreffende gegevensbescherming moet de DPO betrokken worden om zijn advies te vormen en dit naar de business over te brengen.

De aangestelde persoon moet ook voldoende middelen (financiële, tijd, …) krijgen om zijn kennis te onderhouden en zijn taken naar behoren te kunnen uit voeren.

Naast de controlerende, informerende en adviserende rol heeft de DPO ook de taak toe te zien op de naleving van GDPR, het beleid van de controller en de bewustmaking en opleiding van het betrokken personeel en moet de DPO met de Gegevensbeschermingsautoriteit samen werken.

De aangewezen DPO is ook het contactpunt voor zowel de toezichthoudende autoriteit maar ook voor de data subjects. Daarom is het ook noodzakelijk dat de contactgegevens van de DPO kenbaar gemaakt worden op de website.

6 Wat bij verwerking door een externe processor?

Een verwerkingsverantwoordelijke kan ook de keuze maken om de verwerking van gegevens uit te besteden aan een externe processor. Hier hangen opnieuw wat voorwaarden aan waar zowel de processor als controller aan moeten voldoen. Dit kort hoofdstuk zal deze controller-processor relatie verduidelijken.

6.1 Criteria bij het aanstellen van een processor

Indien een controller (verwerkingsverantwoordelijke), een externe partij aanstelt moet de verantwoordelijke kiezen voor een verwerker/processor die gegevensbescherming garandeert gelijkwaardig aan de GDPR-verordening.

Het is ook aangeraden om te kiezen voor een processor die minstens dezelfde technische en eventueel organisatorische maatregelen neemt op vlak van beveiliging en beleid om de persoonsgegevens van de betrokken personen veilig te stellen.

Het is ook van uiterst belang om een Data Processing Agreement (DPA) of een contract af te sluiten die standaard clausules bevat die de garantie biedt dat op een correcte manier met de persoonsgegevens gewerkt zal worden.

De minimumzaken die opgenomen moeten worden in zo'n contract zijn:

- het doel van de verwerking,
- het type van verwerking,
- welk soort persoonsgegevens zullen verwerkt worden,
- categorieën van de betrokken personen (bv. kinderen, werknemers, …)
- de verplichtingen en rechten van de controller.

6.2 Verplichtingen van de processor

Ook de processors of verwerkers die in opdracht werken, hebben onder de GDPR-verordening enkele verplichtingen.

- Een processor mag niet zomaar een nieuw contract met een zogenaamde 4e partij aangaan. Hiervoor heeft hij de schriftelijke toelating van de verwerkingsverantwoordelijke nodig. Ook bij het veranderen van "subcontractor" of veranderingen in het contract moet hij de verwerkingsverantwoordelijke inlichten zodat deze zich eventueel kan verzetten hiertegen.

Case Facebook – Cambridge Analytica – Aleksandr Kogan
Aleksandr Kogan, een lector psychologie en data science aan de universiteit van Cambridge, verzamelde gegevens door een persoonlijkheidsquiz-applicatie die via Facebook werkte. Deze applicatie vroeg toestemming van de betrokken persoon die deze quiz invulde om zijn gegevens te verwerken. Maar door de gebruiksvoorwaarden van Facebook, gaf de betrokken persoon, zonder dit zelf te weten, toestemming in naam van zijn vrienden en kennissen om ook hun gegevens te verwerken.

Reflectie: Facebook is hier overduidelijk verwerkingsverantwoordelijke net als Aleksandr Kogan. Facebook voorzag hier functionaliteit die niet wettelijk is door een persoon toestemming te geven in naam van zijn vrienden. **Toestemming is altijd persoonlijk.**

Nadien verkocht Aleksandr Kogan deze data aan Cambridge Analytica dat op zijn beurt software bouwde om de politieke overtuigingen te voorspellen. Dit gebeurde zonder dat de betrokken personen hiervan op de hoogte waren en zonder dat hier toestemming werd voor gegeven. Deze gegevens werden uiteindelijk ingezet om doelgerichte propaganda te versturen tijdens de Amerikaanse verkiezingen om twijfelende kiezers te manipuleren en op Donald Trump te stemmen. Maar er is ook bewijs gevonden dat Cambridge Analytica betrokken was bij de Brexit campagne.

Reflectie: Aleksandr is hier ook verantwoordelijke omdat hij zelf het doel voor de verwerking vooropstelde. Ook verkocht hij **zonder toestemming** de gegevens aan een andere partij.
Cambridge Analytica op zijn beurt verwerkte deze gegevens **zonder toestemming** om zo doelgerichte Donald Trump campagne te tonen aan gebruikers op Facebook. Aangezien politieke overtuiging een bijzondere categorie van persoonsgegevens is en er sprake was van grootschalige profiling, had Cambridge Analytica zelfs **uitdrukkelijke toestemming** moeten vragen voor dit soort bewerking uit te oefenen.

Wat nu?

- De Britse Gegevensbeschermingsautoriteit heeft reeds een raid uitgevoerd op Cambridge Analytica om zoveel mogelijk bewijsmateriaal te verzamelen. Er komt dan ook een verder onderzoek naar de feiten.
- Het Britse parlement wil dat Mark Zuckerberg zich komt verantwoorden.
- Senators van de US roepen Mark Zuckerberg op om zich te verantwoorden voor het Congres.
- Het Europese Parlement zal ook een onderzoek opstarten om te kijken of er gegevens van Europese burgers misbruikt werden.
- Er komt ook een onderzoek naar mogelijke inmenging bij de verkiezingen van Kenya in 2013.

Hoe reageren de partijen zelf?

- Zowel Facebook als Cambridge Analytica zeggen dat ze niets verkeerd hebben gedaan
- Facebook zegt dat de persoonsgegevens op een legale manier verzameld werden maar dat Cambridge Analytica die niet verwijderde wanneer dit gevraagd werd. (Dit insinueert dat Facebook al langer van het lek wist maar dit dus niet publiek communiceerde).
- Een woordvoerder van Facebook zei dat Kogan deze gegevens niet mocht doorgeven aan een andere partij die commerciële doeleinden voor ogen had.
- Hieraan voegden ze toe dat het tegen de regels van Facebook zelf is om gegevens van vrienden van de gebruikers te delen.
- Cambridge Analytica verdedigt zichzelf door te zeggen dat ze dat het wel de gegevens op vraag van Facebook had verwijderd.

Overduidelijk wordt dit verhaal vervolgd.

- Vanzelfsprekend moet een verwerker die in opdracht van een controller werkt, zich houden aan de contractuele overeenkomst. En enkel verwerkingen uitvoeren in opdracht van de verwerkingsverantwoordelijke. Indien hier een inbreuk op zou zijn kan de verwerker toch als controller beschouwd worden om op die manier verantwoordelijk gesteld te worden.

- Ook een processor moet een register van verwerkingsactiviteiten bijhouden. Een voorbeeld van dergelijk register kan u terugvinden onder Bijlage 4: Voorbeeld register van verwerkingsactiviteiten.
- Als de verwerker een inbreuk met betrekking tot persoonsgegevens opmerkt moeten ze dit zo snel mogelijk melden bij de verwerkingsverantwoordelijke.

7 De impact van GDPR op IT Governance & IT Security

"It is not simply a case of having a set of procedures and processes, nor is it just about having controls in place. Reliance on a poor control is often worse than having no control at all. [The trustees must have] … a clear understanding of the business and what can go wrong." - Tony Rawlins - (2001)

De GDPR spreekt vaak over security en privacy by design. Dit hoofdstuk haalt aan wat de impact zal zijn op IT-security gerelateerde processen. Maar ook hoe dit doel van de GDPR kan bereikt worden.

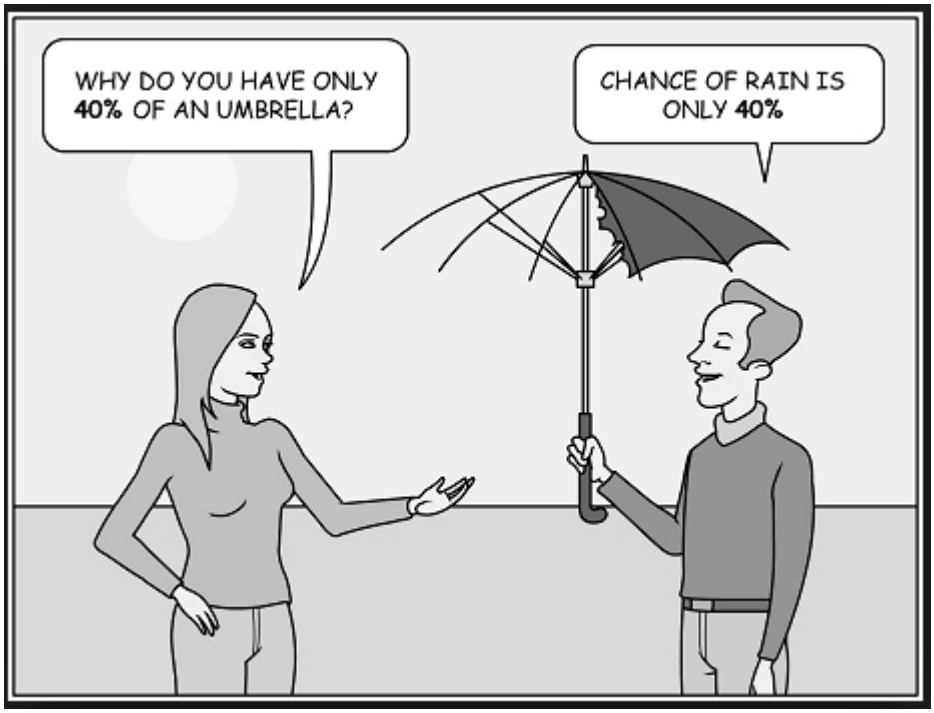
7.1 Wat is IT Governance?

IT governance is een framework dat de IT-strategie koppelt aan de business strategie. Door een sterk framework op te bouwen met meetbare resultaten kan er controle gevoerd worden op de strategie van het bedrijf en of de vooropgestelde doelen bereikt worden. Dit framework kan bestaan uit verschillende policies en procedures die gevolgd moeten worden.

7.2 Mentaliteitswijziging

Aangezien de controller de verantwoordelijkheid zal dragen binnen de onderneming, is hij verantwoordelijk voor zijn personeel en hoe deze omgaan met persoonlijke gegevens. Er zal ook op lagere niveaus in een onderneming rekening moeten gehouden worden met de GDPR. Het is dus de verantwoordelijkheid van de controller om een nieuwe mentaliteit te kweken onder de werknemers zodat iedereen beseft wat de gevolgen kunnen zijn van het niet naleven van deze wetgeving. Dit kan gerealiseerd worden door een sterk of versterkt (IT) beleid.

7.3 Riskmanagement



Bij de ingang van de GDPR-verordening zal de verantwoordelijkheid van het aantonen dat de wet nageleefd wordt op de schouders van de verwerkingsverantwoordelijke vallen. De GDPR is ook opgebouwd vanuit het standpunt van een risico gebaseerde aanpak.

Hierdoor moet de verwerkingsverantwoordelijke zelf de risico's gaan bepalen van zijn verwerkingen als die betrekking hebben op persoonsgegevens. De GDPR laat je vrij hoe je dit risico bepaalt, maar verwerkingen die een hoog risico inhouden voor de betrokken personen moeten aangegeven worden aan de Gegevensbeschermingsautoriteit.

Om een extra hulp aan te bieden om het risico te bepalen heeft werkgroep "Working Party 29" hiervoor aanvullende documenten voorzien. Tijdens mijn stage heb ik deze documenten dan ook gebruikt om een risicoanalyse uit te werken zodat op een snelle en duidelijke manier de meest kritische applicaties en derde partijen voorgesteld kunnen worden om verdere maatregelen te kunnen nemen naargelang het risico.

7.3.1 Basis van de toegepaste risk assessment methodologie

Zoals hierboven gezegd gebruikte ik een van de "Working Party 29" documenten als leidraad om tot een risicoanalyse formule te komen. Het gebruikte document hiervoor heet "Recommendations for a methodology of the assessment of severity of personal data breaches".

Strikt genomen spreekt de GDPR slechts van persoonsgegevens en persoonsgegevens van bijzondere categorieën. (Zie Bijlage 1: Categorieën van persoonsgegevens). Hierdoor vallen bepaalde categorieën die sensitiever aanvoelen buiten beschouwing en worden ze aanzien als geen gevoelig gegeven, denk hierbij aan gedragsgegevens, locatiegegevens, financiële gegevens…

Deze werkgroep spreekt daarom van 4 categorieën om een specifieker onderscheid te maken tussen persoonsgegevens. Het gevolg is dan ook dat er een specifiekere risicobepaling kan gemaakt worden op basis van deze categorieën van persoonsgegevens.

Dit document kent een basis score toe aan categorieën van persoonsgegevens naargelang de gevoeligheid ervan zoals gezien in onderstaande tabel.

Categorie van verwerkte gegevens	Basis score
Simple data	1
Behavioral data	2
Financial data	3
Sensitive data	4

Om een duidelijker beeld te scheppen wat er allemaal binnen deze categorieën van persoonsgegevens valt geef ik hieronder enkele voorbeelden.

Simple data:

- Biografische gegevens
- Contactgegevens
- Naam en voornaam
- Gegevens over schooling
- Gegevens over samenstelling van het gezin
- Professionele ervaring

Behavioral data:

- Locatiegegevens
- Gegevens met betrekking tot persoonlijke voorkeuren
- Levensgewoontes

Financial data:

- Inkomen
- Financiële transacties
- Bankafschriften
- Gemaakte investeringen
- Kredietkaarten
- Gegevens in verband met de sociale welvaart

Sensitive data:

Dit zijn dan de uiteindelijke gegevens die bij de GDPR onder gegevens van bijzondere categorie vallen zoals gezien in Bijlage 1: Categorieën van persoonsgegevens, maar ik geef ook nog enkele voorbeelden mee.

- Medische gegevens
- Gegevens met betrekking tot het seksuele leven
- Politieke voorkeuren

7.3.2 Dataprocessing context

Omdat de context waarin persoonlijke gegevens verwerkt kan worden een grote impact kan hebben op het daarbij horende risico, moet hiermee rekening gehouden worden zodat een correcte objectieve score kan bepaald worden.

In dit proces gaan we basis score gaan aanpassen naargelang de context waarin de persoonsgegevens verwerkt worden.

De score kan **verlaagd** worden als in de context van de verwerking het risico lager ingeschat kan worden.

- Financiële gegevens hebben een basis score van 3 maar kan herleid worden naar 2 als deze enkel bankrekeningnummers betreft en de financiële status van de betrokken persoon niet kan uit afgeleid worden.

De score kan **verhoogd** worden als in de context van de verwerking het risico hoger ingeschat wordt.

- Simpele gegevens hebben een basis score van 1 maar kan opgetrokken worden naar 3 als door de context van verwerking vermoedens over de gezondheid van de betrokken persoon kunnen gemaakt worden. Denk aan een lijst van contactgegevens van patiënten die onlangs een hartspecialist hebben bezocht.

Type of personal data	Working party 29 category	Processing risk in context
Identification data (Name, titles, address, phone, email, …)	Simple data	1
Electronic identification data (IP address, cookies, …)	Behavioural data	2

Electronic localization data (GSM, GPS, ...)	Behavioural data	2
Biometric identification data	Sensitive data	4
Financial identification data (card numbers)	Financial data	2
Financial transactions	Financial data	3
Payroll data (salaries)	Financial data	3
Personal characteristics (age, gender, birthday, …)	Simple data	1
Personal characteristics regarding immigration	Simple data	4
Personal characteristics regarding physical attributes (height, weight, hair color, ...)	Simple data	2
Life habits	Behavioural data	2
Life habits with impact on health	Behavioural data	4
Psychic data	Sensitive data	4
Leisure activities and interests	Behavioural data	2
Consumption habits	Behavioural data	2
Data regarding work (time clock)	Behavioural data	3
Video, audiodata	Behavioural data	3
Sensitive data regarding sexual life and sexual preferences	Sensitive data	4
Health data concerning identifiable persons	Sensitive data	4

Bovenstaande figuur is een voorbeeld van hoe gegevens aangepast kunnen worden aan de context van verwerking. Merk op dat dit slechts een voorbeeld is, de GDPR laat je vrij om zelf categorieën te bepalen.

7.3.3 Geïmplementeerde securitymaatregelen

Volgens de GDPR mag je ook het risico aanpassen naargelang de geïmplementeerde securitymaatregelen. Hiervoor heb ik een schaal voorzien naargelang hoe goed een applicatie of infrastructuur beveiligd is, of naargelang welke beveiligingsimplementaties een derde partij heeft voorzien in de dataprocessing agreement.

Omdat deze schaal moeilijk te categoriseren is en aanvaardbare beveiligingsmaatregelen verschillen naar gelang de aard van verwerking, zou deze bepaling moeten gebeuren aan de hand van audits.

Security Risk category	Risk scale
Strong security implemented	0,25
Best practice security implemented	0,5

Basic security implemented	0,75
Unknown	1,5
No security measures implemented	1,75
Known security issues	2

7.3.4 Locatie van de gegevensverwerking

Een verder belangrijk aspect volgens de GDPR is waar de gegevens verwerkt of opgeslagen worden. Gegevensverwerkingen die onder de GDPR vallen moeten binnen de EEA (European Economic Area) gebeuren of in een land dat op de witte lijst staat die de garantie op een adequate gegevensbescherming bieden (Zie Bijlage 7: Landen op de witte lijst voor adequate gegevensbescherming). Ik voorzag hiervoor volgende risico schaal.

Location	Risk scale
European Economic Area	1
Whitelisted Countries	1
Outside European Economic Area	2
Unknown	1,5

7.3.5 Het aantal data subjects

In deze risicoanalyse die ik opgebouwd heb houd ik ook rekening met het aantal betrokken personen bij de gegevensverwerking. Hieraan heb ik op zijn beurt een risico schaal gekoppeld. Deze waarden kunnen op hun beurt aangepast worden aan de specifieke noden, dit is slechts een voorbeeld.

Volume	Risk scale
<1000	1
<10000	1,5
>10000	2
Unknown	1,25

7.3.6 Het resultaat

Het uiteindelijke resultaat wanneer je alle uitkomsten met elkaar vermenigvuldigt krijg je een waarde tussen 1 en 24. Hiertussen heb ik een schaal gemaakt met het ingeschatte resultaat en risico van de verwerking.

Result lower than	Risk
5	Low
10	Medium
24	High

7.3.7 De gevolgen van GDPR op IT Security en IT Governance

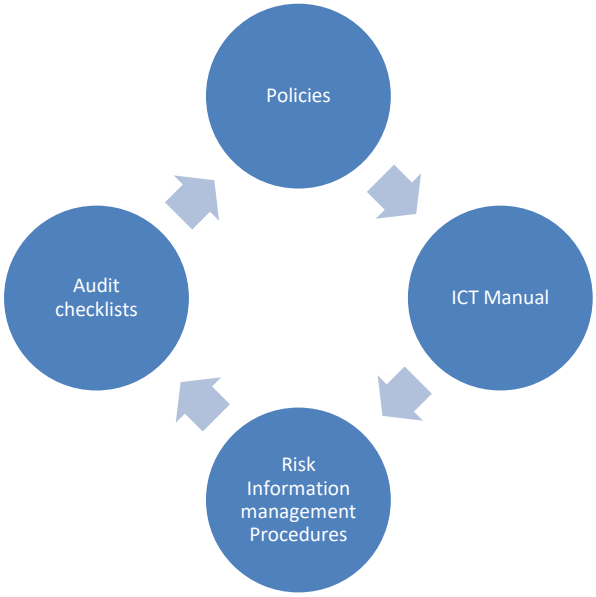
Aangezien de verantwoordelijkheid om conformiteit aan te tonen nu rust op de schouders van de controller zal dit voor verbeteringen zorgen wat betreft de algemene veiligheid van de IT-infrastructuur en de manier waarop met persoonsgegevens omgegaan worden.

De GDPR spreekt dan ook veelvuldig van security en privacy by design/default. Dit is het concept waarbij IT-security en privacy kernbegrippen worden bij het starten van nieuwe verwerkingen waarbij persoonsgegevens betrokken zijn of de veiligheid van waar deze gegevens opgeslagen worden. Een andere interpretatie van dit begrip is dat de industrie standaarden op vlak van gegevensbescherming en cyberveiligheid moeten worden gehanteerd.

Door dat het gegeven dat er betere veiligheid vereist is, zal er ook een betere IT Governance tot stand komen om audits op de IT-infrastructuur uit te voeren en op zijn beurt aandachtspunten aan het licht te brengen waar de beveiliging kan verhoogd worden.

7.4 Voorbeeld van een Risk Information Management framework

Na het inschatten van de risico's is het belangrijk om de correcte maatregelen te nemen. Een belangrijk aspect zit dan ook in IT Security Management. Tijdens mijn stage bij Kinepolis heb ik een eenvoudig maar duidelijk framework opgezet om het IT beleid binnen de Kinepolis Group te versterken. Dit framework bestaat uit 4 delen en is cyclisch (zoals hieronder voorgesteld):



1) **Policies:** De policies zijn de basis uitgang van framework. Dit zijn de volledig tot in detail uitgeschreven beleidsregels en richtlijnen.
2) **ICT Manual for end-users:** Het ICT-manual of handboek bevat de belangrijkste zaken die de werknemers moeten weten over een policy. Dit is een document geschreven naar niet technische mensen en is dus zeer begrijpbaar.
3) **Risk Information Management (RIM) procedures:** Risk information management procedures zijn de vastgelegde procedures die moeten gevolgd worden om de policy af te toetsen aan de werkelijkheid. Hierin staat hoe en hoe vaak een policy gecontroleerd moet worden.
4) **Audit checklists:** dit zijn de rapporten die het gevolg zijn van een RIM-controle. Deze checklists worden afgetoetst met de policies en indien nodig geëscaleerd.

7.5 Incident of breach response plan

Helaas moeten bedrijven altijd bewust zijn dat een sterk IT beleid niet altijd genoeg is. Er is altijd een kans dat het fout gaat, IT security kan nooit 100% gegarandeerd worden. Daarom moet ook met noodsituaties rekening gehouden worden. Een belangrijk document die nodig is voor de GDPR is een plan voor een worstcasescenario, namelijk wanneer er een security en/of data incident of breach plaatsvond. Dergelijk document heet een Incident (of Breach) Response plan. Dit plan moet helpen om het bedrijf zo snel mogelijk weer 100% functioneel te krijgen, en om te voldoen aan de wettelijke verplichtingen van de GDPR.

Er is ook een duidelijk verschil tussen een incident en een breach (inbreuk). Een inbreuk is altijd een incident, maar een incident is niet altijd een inbreuk. Deze kunnen tot een bepaald niveau vrij bepaald worden. Hieronder wat voorbeelden die duidelijk maken wat het verschil tussen een incident en inbreuk is. Dergelijke onderverdeling is zeer belangrijk om te bepalen wanneer er melding moet gemaakt worden bij de Gegevensbeschermingsautoriteit.

Incidenten

- Een mail naar een verkeerde ontvanger versturen
- Afgedrukte bestanden met persoonlijke gegevens in de printer laten liggen
- Verliezen van een USB-stick

Inbreuken

- Diefstal van een laptop met persoonlijke gegevens
- Hacking met gevolg diefstal van gegevens of schade aan databases of systemen die persoonlijke gegevens bewaren
- Een boze ex-werknemer die een data dump online gooit

Dergelijk plan is bedoeld om de schade door een security of data gerelateerd incident of een inbreuk naar de business toe te beschermen, maar ook om de duur van het herstel en de bijhorende kosten hiervan te beperken.

Bij een security of data breach incident of inbreuk is het van belang dat er goede communicatie is. Daarom is er een response team nodig om de situatie af te handelen en het probleem op te lossen aan de hand van een response plan.

Volgende stappen kunnen helpen bij het opstellen van dergelijk plan:

1. **Stel een response team samen**
   De eerste stap is om een team bijeen te roepen en rollen te verdelen wie welke verantwoordelijkheid zal opnemen om het incident of de inbreuk af te handelen. Betrek hier ook zeker de Data Protection Officer of de verantwoordelijke voor gegevensbescherming indien een DPO niet verplicht is. Andere rollen die nuttig zijn voor het response team zijn onder meer **Legal, IT, Security Operations, Communication, Helpdesk.**

2. **Onderzoek van het incident**

   Het is belangrijk om te weten wat de precieze omstandigheden zijn zodat de juiste verdere stappen kunnen genomen worden. Er moet gekeken worden of het incident leidde tot een inbreuk betreffende persoonsgegevens. Indien er sprake is van diefstal hoort dit ook gemeld te worden aan de juiste instanties.
   Bij een security incident is het belangrijk dat de nodige stappen genomen worden om dit op te lossen. Hiervoor kan een intern security incidentproces opgemaakt worden om de opvolging van het probleem te garanderen.

3. **Personal data breach risk and impact assessment**

   Indien er sprake was van een inbreuk met persoonsgegevens is het van uiterst belang om een risico en impact analyse uit te voeren.
   In dit verder onderzoek moet ook onderzocht worden:
   - wat de oorzaak is van het gegevenslek,
   - hoeveel personen betrokken zijn,
   - of er een risico is op de rechten en vrijheden van de betrokken personen,

- de aard van gelekte of gestolen gegevens zoals sensitieve gegevens,
- of er cryptografische gegevensbescherming was zodat de data van onleesbare aard is (rekening houdend of het gebruikte algoritme een hedendaagse standaard is),
- of er andere partijen bij de inbreuk betrokken waren.

4. **Contacteer de Gegevensbeschermingsautoriteit en eventueel de betrokkenen**

   De GDPR heeft ook artikels voorzien die de melding van een inbreuk betreffende persoonsgegevens onder bepaalde omstandigheden verplichten. (Zie Bijlage 3: Schema rapporteren van inbreuken betreffende persoonsgegevens).

   Dit is een belangrijk element van de incident response procedure en mag zeker niet ontbreken, het is dan ook een belangrijke rol die toegekend moet worden aan een persoon in het incident response team om de communicatie aan te voeren met de Gegevensbeschermingsautoriteit, dit zal in de meeste gevallen de Data Protection Officer zijn.

   Verder is er ook de nood aan een procedure die gevolgd kan worden hoe de communicatie naar de betrokken personen zal verlopen.

5. **Bijhouden van een intern incident register**

   Elk incident en elke inbreuk betreffende IT-security en persoonsgegevens moet bijgehouden worden in speciaal daarvoor voorzien register. Elke regel bevat uitleg over het incident, genomen of gepland maatregelen en of de Gegevensbeschermingsautoriteit werd ingelicht.

6. **Evalueren van de interne policies**

   Na een incident of data breach is het nodig om te controleren of de policies volstaan om in de toekomst dergelijke incidenten te voorkomen. Er kan ook nagedacht worden om nieuwe policies van kracht te brengen en zo een sterk evolueerde cyclus te ontwikkelen.

8 De impact van GDPR op IT-development

8.1 GDPR, Big Data en artificiële intelligentie

8.1.1 Wat is "big data"?

Big data is het totaalbegrip dat spreekt over gigantische data sets waarop statistische analyses worden uitgevoerd, om op deze manier patronen en trends te herkennen. Het resultaat van een dergelijke analyse kan voor verschillende doeleinden zoals marketing.

Een van de problemen met "big data" is dat door het grote volume aan gegevens die binnenkomen op korte termijn en de variatie van de gegevens hier moeilijk analyses kunnen op gemaakt worden.

8.1.2 Wat is "artificiële intelligentie"?

Door de grootte van deze data sets aangehaald hierboven, moet er naar alternatieve manieren gekeken worden om snelle (liefst in real-time) analyses te maken. Artificiële intelligentie kan hier de oplossing bieden.

Artificiële intelligentie is een effectieve manier om snelle, objectieve operaties uit te voeren op gegevenssets. Deze operaties kunnen verschillen van het klasseren van gegevens, conclusies trekken uit grote datasets of predictie modellen bouwen. Maar ook kan artificiële intelligentie profielen gaan bouwen gebaseerd op interesses en persoonsgegevens.

8.1.3 De link met GDPR

Zoals in hoofdstuk 4"Welke impact heeft de GDPR op u en mij als data subjects?" aangehaald krijgen de betrokken personen het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming inclusief het opmaken van een profiel van deze betrokken persoon.

Dit kan echter gevolg hebben op het Business Intelligence departement van de onderneming. Hieronder kan je enkele aanbevelingen vinden die helpen om ook het big data gedeelte binnen de onderneming compliant aan de GDPR te krijgen.

- Zorg dat Business Intelligence niet gaat profileren tot 1 bepaald individu, maar dat het trekken van gevolgen herleid wordt tot een niet herleidbare groep van personen. Dit kan op basis van categorieën zoals "Jongeren tussen 13 en 17".

- In principe heeft Business Intelligence geen nood aan de persoonsgegevens in de eerste instantie. Omwille van data minimalisatie en als extra securitymaatregel kan er een vorm van pseudonymisatie of anonimisering gebruikt worden op de dataset die ter beschikking gesteld wordt voor de statistische doeleinden.

- Ga transparant om met deze gegevens, vertel de betrokken personen hoe de gegevens verzameld werden, gebruikt worden en wat de mogelijke gevolgen zijn van de verwerking. Dit kan omschreven worden in een privacy statement die geplaatst wordt op de website van de onderneming.

8.2 IT-ontwikkeling en de GDPR

Een van de vele onduidelijkheden in de GDPR is welke veranderingen er moeten gebeuren in het proces van IT-ontwikkeling. Hier maak ik graag nogmaals de link naar het hoofdstuk "De impact van GDPR op IT Governance & IT Security".

Dit omdat er voor het ontwikkelen van nieuwe applicaties of andere toepassingen in het IT-gebied binnen een onderneming toch wel duidelijke richtlijnen moeten worden vooropgesteld.

Ik zal hier enkele ideeën schetsen die opgenomen kunnen worden om het IT-beleid uit te breiden.

8.2.1 Scheiding van omgevingen

Vaak worden in ondernemingen verschillende stappen genomen in het ontwikkelingsproces van nieuwe toepassingen of uitbreidingen van de reeds bestaande (software)architectuur. Deze zijn **Development**, **Testing**, **Productie**.

Een beleid kan zijn dat ontwikkelaars geen toegang krijgen tot de test- en productieomgeving. Hierdoor krijgen ze al geen toegang tot eventuele persoonsgegevens die niet strikt noodzakelijk zijn voor de uitvoering van hun dagdagelijkse taken.

En op die manier ken verder geredeneerd worden, het principe van noodzaak voor de uitvoering van de dagdagelijkse job. Verleen enkel toegang aan personen die toegang nodig hebben aan die omgevingen.

8.2.2 Changemanagement

Een andere policy kan zijn dat voor er een wijziging in de IT-infrastructuur van start gaat, er een procedure moet doorlopen worden.

1) Aanvraag/goedkeuring budget voor de wijziging of het project
2) Kick-off vergadering met betrokken partijen (developers, DPO, Security Officer, …)
3) Start ontwikkeling in de development omgeving
4) Quality & Assurance testing in de test omgeving
5) Security testing in de test omgeving
6) Aanvraag voor overdracht naar de productie omgeving door middel van een “Change Request Approval Form”.
7) Deploy de wijziging of project naar productie

Voor een voorbeeld van een “Change Request Approval Form”, zie “Bijlage 8: Change Request Approval form”.

Door dat dit proces meer testen vergt maar ook de toelating van de betrokken stakeholders, zal dit er voor zorgen dat de ontwikkeltijd van projecten mogelijks zal verlengen.

8.2.3 Opleiding en awareness

Ook personen die niet rechtstreeks in contact komen persoonsgegevens zoals ontwikkelaars, moeten goed bewust zijn wat GDPR precies betekent. Daarom is het van cruciaal belang dat ze correct opgeleid worden zodat men geen overtredingen tegen de GDPR in productie gaat plaatsen. De juiste contactpersonen aanduiden waar IT ontwikkelaars hun vragen kwijt kunnen is dan ook zeer cruciaal.

8.3 Proces optimalisatie

De GDPR verplicht bedrijven om hun processen in kaart te brengen, specifieker de processen die in aanraking komen met persoonsgegevens. Door alles in kaart te brengen ontdekt de onderneming waar er gebreken zijn aan geschreven procedures en/of waar er verbeteringen kunnen worden geïmplementeerd.

Enkele voorbeelden waar een procesmatige manier van werken helpt om compliant te zijn aan GDPR.

- Het beantwoorden van **klachten op sociale media**. Als dit gebeurt via het sociale medium zelf is er **geen controle** naar waar deze data precies gaan en hoe lang deze worden bijgehouden. Er kan beter geopteerd worden voor **software die logs kan bijhouden** met een ingestelde **retentieperiode**. Op deze manier kan er een beter uitgeschreven procedure gemaakt worden over hoe er moet gecommuniceerd worden naar boze klanten toe.

- Een tijd terug had Argenta enkele **problemen na een update**. Hierdoor waren **geen financiële transacties mogelijk**, dit een week lang. Omdat Argenta **geen procedure** had voor deze risico’s stuurden ze **mails** uit met de vraag om manueel de overschrijvingen te doen mits je de **betaalgegevens doorgaf**. Deze methodiek was vanzelfsprekend zeer interessant voor cybercriminelen die de inhoud van de mail kopieerden en op deze manier **“phishing”-mails** uitstuurden. Overduidelijk kan hier een beter proces voorzien worden. Een alternatief kan zijn om een webpagina op te zetten die op zen minst gebruik maakt van SSL en na afloop van de problematiek een automatisch proces die de opgevraagde gegevens verwijderd.

Philippe De Backer haalde dit indirect ook aan in mijn interview. Hij is van mening dat de GDPR meer dan alleen maar een nieuwe wetgeving is. Hieronder een stuk uit in mijn interview die dit aantoont. Het volledige interview kan terugvonden in Blog 3: Interview with the Belgian State Secretary for privacy Philippe De Backer.

"But I like to see it more as an opportunity for companies to gain a clear view on the data they possess, to better protect their environments and the personal data within it. This will lead to a higher consumer trust, and thanks to GDPR I believe a compliant company will have it easier to gain new clients but also to provide them with a better service."

9 Kritische reflectie

In dit hoofdstuk zal ik kritiek en bemerkingen geven die ik ondervonden heb tijdens mijn onderzoek en mijn stage.

9.1 De GDPR houdt geen rekening met nieuwe technologie

In zijn huidige context houdt de GDPR niet altijd rekening met nieuwe technologische evoluties wat schadelijk kan zijn voor technologische expansie. Hier kunnen we ook van de “kip en het ei”-paradox spreken. Want we kunnen ons ook afvragen of de nieuwe technologie niet heeft rekening gehouden met privacy by default.

Blockchain architectuur

Blockchain in zijn huidige vorm kan niet gebruikt worden voor het opslaan van persoonsgegevens, dit omdat de mogelijkheid om het uitvoeren van de individuele rechten van de betrokkene in het gedrang komt. Je kan namelijk een ‘block’ niet meer aanpassen of verwijderen zonder de ‘ketting’ corrupt te maken.

Er zullen dus duidelijke richtlijnen moeten komen over hoe en voor wat een blockchain kan en mag gebruikt worden.

Een manier hier kan zijn om de mogelijks betrokken persoonsgegevens “off-chain” te bewaren in een geëncrypteerde vorm. Wanneer een recht op vergetelheid uitgeoefend wordt zou de sleutel vernietigd kunnen worden. Dit is natuurlijk niet hetzelfde aangezien de data wel nog bewaard opgeslagen is. Rechtspraak zal moeten uitwijzen of dit een voldoende correcte manier is om deze techniek “GDPR-compliant” te kunnen noemen.

Machine learning en AI

Hier heb ik toch wat bedenken bij het interview met staatssecretaris Philippe De Backer, waarin hij me vertelde dat hij profiling en automatische besluitvorming enkel mogelijk ziet bij expliciete toestemming van de betrokken persoon.

Ik denk dat dit statement moet genuanceerd worden omdat er verschillende gradaties van profielvorming zijn. Bij Kinepolis, Telenet en Proximus gaat dit slechts over het bijhouden van filmvoorkeuren om in kader van gerechtvaardigd belang vanuit het bedrijf nieuwsbrieven te sturen, deze uitkomst van deze verwerking wordt ook niet op individueel niveau gebruikt.. Maar op deze manier van classificatie krijgen de betrokken personen enkel mails over hun eigen interesses.

Netflix en Spotify doen hier trouwens exact hetzelfde om films, series en muziek voor te stellen gebaseerd op wat je reeds gezien en beluisterd hebt.

Mijn mening is dat profielvorming en automatische besluitvorming gebaseerd moet worden op expliciete toestemming wanneer deze concrete impact hebben op het leven van een betrokkene. Denk hierbij aan automatische sollicitatierondes, premies voor verzekeringen, …

Anderzijds is het ook belangrijk dat betrokken personen zich kunnen beroepen op hun rechten onder de GDPR. In bovenstaande gevallen zou recht op bezwaar van de verwerking kunnen ingeroepen worden.

9.2 Verschillen in de wetgeving

9.2.1 Vingerafdrukken voor tijdsregistratie

De GDPR laat de uitvoerende wetgeving vrij op nationaal niveau. Hierdoor kunnen toch grote verschillen zijn in de uitvoering van de GDPR; het hele punt wat GDPR net wou vermijden. Een van deze voorbeelden is dat Nederland althans de registratie van vingerafdrukken bedoelt voor het registreren van werktijden **volledig** heeft verboden (zelfs onder grondslag expliciete toestemming, aangezien in een werkrelatie er geen sprake kan zijn van toestemming), terwijl in België hierover nog geen standpunt over is ingenomen.

Dit kan nefaste effecten hebben op bedrijven die internationaal dezelfde systemen gebruiken voor het registreren van de werktijden van hun werknemers. Zeker als dit een nieuwe investering was om het systeem gebruiksvriendelijker te maken, hierdoor hoeven ze geen code te onthouden of een pas bij te houden die bovendien kan verloren worden.

Maar een andere kwestie is dat voorafgaand aan de GDPR, de verwerking van vingerafdrukken voor het registreren van werktijden wel toegelaten is. Dit kon namelijk onder legitiem belang, want een vingerafdruk is een sterk systeem om fraude van de werktijden te voorkomen. Een badge of pincode kan namelijk makkelijk worden doorgegeven.

Ik ben van mening dat hier de GDPR een uitzondering voor moest voorzien. Het verwerken van vingerafdrukken is namelijk wel mogelijk voor toegangscontroles wat ook in het belang is van een onderneming. Het bestrijden van fraude lijkt mij toch een gerechtvaardigd belang van een onderneming. Zeker indien er gebruik gemaakt kan worden van hashing algoritmes zoals een “fuzzy-vault”-algoritme. Dergelijk algoritme kan je vergelijken met het opslaan van paswoorden. Hierdoor kan de vingerafdruk niet achterhaald worden door mogelijks geïnteresseerde partijen.

Bovendien is er hier ook een manier waarop je dergelijk systeem kan beveiligen. Hiervoor verwijs ik graag naar de voetnoot.[5]

9.2.2 Verschillende nuances in de vertaling van GDPR

Niet alle vertalingen van de GDPR zijn even goed geslaagd, soms zit er een verschil in nuance maar de Roemeense vertaling heeft soms een totaal verschillende betekenis dan de originele teksten.

Enkele van deze fouten zitten ook in de Nederlandstalige vertaling. Zo staat er bijvoorbeeld dat een Data Protection Officer moet rapporteren aan de hoogste manager in plaats van het hoogste management level. Dit zou in principe willen zeggen dat de Nederlandse en Belgische autoriteiten boetes kunnen opleggen indien de DPO niet direct aan de CEO rapporteert. Een zeer interessant artikel over deze vertalingsfouten kan je vinden in de voetnoot van deze pagina.[6]

Ik kreeg ook enkele documenten te bezichtigen die dit beamen. Jammer genoeg door de aard en gevoeligheid kan ik deze niet bespreken. Ze beamen anderzijds wel dat er verschillen mogelijk zijn in de nationale kaderwetten.

---

[5] Hashing van vingerafdrukken: *https://cubs.buffalo.edu/images/pdf/pub/symmetric-hash-functions-for-secure-fingerprint-biometric-systems.pdf*
[6] GDPR lost in translation: *https://iapp.org/news/a/gdpr-lost-in-translation/*

9.3 Het nationaal bepalen van de DPA

Philippe De Backer haalde aan dat het mogelijk problematisch is dat de autoriteit persoonsgegevens aangesteld wordt op nationaal niveau. Ik geef hem hier volledig gelijk in. Dit kan namelijk leiden tot een inconsequente uitvoering van de GDPR-verordening.

Ook is de GDPR een Europese verordening en vind ik het persoonlijk zonde dat hiervoor geen Europees orgaan wordt aangesteld als DPA.

Verder heb ik toch ook wat commentaar naar de Belgische privacy commissie, de zaken die ze aanbieden zijn van kwaliteit toch heel wat minder dan wat bv. ICO, de Britse Gegevensbeschermingsautoriteit, aanlevert. De Britse autoriteit persoonsgegevens levert zeer bruikbare documenten en adviezen aan om compliant te worden aan de GDPR-verordening. Een oplossing zou kunnen zijn dat er toch bepaalde minimumnormen en regelgevingen vanuit Europa moeten gemaakt worden die de Gegevensbeschermingsautoriteiten moeten handhaven.

9.4 Lijst van landen die adequate bescherming bieden

Data delen buiten de Europese Unie is principe niet toegelaten. Dit is wel toegelaten mits het land waar de andere entiteit zich bevindt, op de lijst van adequate landen staat. Hier heb ik toch wat kritiek omdat de Verenigde Staten hier bij staan. Op dit moment bestaat het US Privacy Shield nog. Maar er is al langer sprake dat deze maatregel niet als adequaat gezien mag worden. Zelf heeft de US niet zo'n zeer strenge privacy wetgeving in vergelijking met de GDPR. Na het interview tussen de senaat en Mark Zuckerburg, een gevolg van het Cambridge Analytica verhaal, ben ik niet overtuigd dat de oudere politici de nodige kennis of wil hebben om een goede privacywetgeving op te bouwen.

10 Conclusies

De GDPR is een wetgeving die zowel nieuwe als reeds bestaande wetgevingen combineert met het doel om mensen beter te beschermen op vlak van gegevensbescherming. Maar de GDPR maakt het ook makkelijker voor bedrijven die in meerdere lidstaten van de Europese Unie actief zijn door een uniforme wetgeving aan te bieden.

De nieuwe wetgeving zal zorgen voor meer rechten en vrijheden voor de betrokken personen. Dit zal ervoor zorgen dat deze personen meer controle krijgen over wat er allemaal mogelijk is met hun persoonlijke gegevens.

Door de GDPR zal de verantwoordelijkheid van het verwerkingsproces altijd vallen op de controller of verwerkingsverantwoordelijke, deze zullen nieuwe plichten krijgen om de veiligheid van persoonlijke gegevens te garanderen, maar ook zal de wetgeving zorgen voor bewustwording dat niet zomaar alles kan en mag met persoonlijke gegevens. De bedoeling is dat dit zal leiden tot een mentaliteitsverandering binnen de onderneming.

De GDPR zal zorgen voor betere contractuele overeenkomsten door het voorzien van standaardcontract clausules. Ook voorziet de wetgeving in middelen om processors verantwoordelijk te stellen indien ze verwerkingen uitvoeren buiten gesloten overeenkomsten.

Het gebied van informatiebeveiligingen zal uitbreiden aangezien de GDPR de verplichting oplegt om standaard rekening te houden met de beveiliging van systemen en de privacy en belangen van de betrokken personen. Er zal meer risico gebaseerd te werk gegaan worden om inbreuken met deze wetgeving te vermijden aangezien er mogelijks hoge boetes aan verbonden zijn.

Deze nieuwe verordening zal ook heel wat aandacht vestigen op de bedrijf gerelateerde processen waar persoonsgegevens bij horen. Dan spreek ik onder andere over hoe IT in een onderneming wordt gemanaged. Maar IT reikt verder dan alleen maar de IT dienst binnen een onderneming. Ook Digital Marketing waarbij IT systemen en processen gebruikt worden zullen moeten herzien worden om een voldoende niveau te halen conform de waarden en regels van de GDPR.

10.1 Slotconclusie

De GDPR is een maatregel om personen beter te gaan beschermen tegen misbruik van hun persoonlijke gegevens waarbij deze verantwoordelijkheid komt te liggen op de verwerkingsverantwoordelijke. Deze verwerkingsverantwoordelijke moet dan ook de veiligheid en privacy van betrokken personen respecteren en daarbij de juiste derde partijen selecteren die eenzelfde of betere garanties bieden. De verwerkingsverantwoordelijke zal ook bereid moeten zijn om mogelijke vragen tot het uitoefenen van de nieuwe verworven rechten te behandelen, maar de verwerkingsverantwoordelijke zal ook acties moeten ondernemen om de nieuwe wetgeving na te leven zoals het herbekijken van de huidige IT gerelateerde bedrijfsprocessen.

11 Bronnen- & literatuurlijst

Art. 2 GDPR – Material scope

Retrieved 14/02/2018 https://gdpr-info.eu/art-2-gdpr/

Art. 3 GDPR – Territorial scope

Retrieved 14/02/2018 https://gdpr-info.eu/art-3-gdpr/

Art. 4 GDPR – Definitions

Retrieved 14/02/2018 https://gdpr-info.eu/art-4-gdpr/

Art. 5 GDPR – Principles relating to processing of personal data

Retrieved 14/02/2018 - https://gdpr-info.eu/art-5-gdpr/

Art. 6 GDPR – Lawfulness of processing

Retrieved 4/03/2018 https://gdpr-info.eu/art-6-gdpr/

Art. 7 GDPR – Conditions for consent

Retrieved 4/03/2018 https://gdpr-info.eu/art-7-gdpr/

Art. 9 GDPR – Processing of special categories of personal data

Retrieved 14/02/2018 - https://gdpr-info.eu/art-9-gdpr/

Art.15 GDPR – Right of access by the data subject

Retrieved 19/02/2018 – https://gdpr-info.eu/art-15-gdpr/

Art.16 GDPR – Right to rectification

Retrieved 19/02/2018 – https://gdpr-info.eu/art-16-gdpr/

Art.17 GDPR – Right to erasure (‘right to be forgotten’)

Retrieved 20/02/2018 -

Art.19 GDPR – Notification obligation regarding rectification or erasure of personal data or restriction of processing

Retrieved 20/02/2018 -

Art.20 GDPR – Right to data portability

Retrieved 20/02/2018

Art.21 GDPR – Right to object

Retrieved 21/02/2018

Art.22 GDPR – Automated individual decision-making, including profiling

Retrieved 20/02/2018

Personal Data Breach Severity Assessment Methodology

Retrieved 16/02/2018 - https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity/at_download/fullReport

Whitecase chapter 9: Rights of data subjects – Unlocking the EU General Data Protection Regulation

Retrieved 21/02/2018 - https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation

Guide to GDPR – Lawful basis for processing

Retrieved 4/03/2018 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Data controllers and data processors

Retrieved 15/05/2018 https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

Art.26 GDPR – Joint controllers

Retrieved 15/05/2018 https://gdpr-info.eu/art-26-gdpr/

Art.28 GDPR – Processor

Retrieved 26/03/2018 https://gdpr-info.eu/art-28-gdpr/

Art.30 GDPR – Records of processing activities

Retrieved 11/03/2018 https://gdpr-info.eu/art-30-gdpr/

Art.33 GDPR – Notification of a personal data breach to the supervisory authority

Retrieved 11/03/2018 https://gdpr-info.eu/art-33-gdpr/

Art.34 GDPR – Communication of a personal data breach to the data subject

Retrieved 15/03/2018 https://gdpr-info.eu/art-34-gdpr/

Pseudonymizing vs anonymization

Retrieved 15/03/2018 http://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/

Guide to GDPR ICO

Retrieved 13/05/2018 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

I-scoop.eu – Right to data portability

Retrieved 13/05/2018 https://www.i-scoop.eu/gdpr/right-to-data-portability/

Case Target Corporation

Retrieved 17/04/2018 https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#20afffdb6668

Case bankieren

Retrieved 14/05/2018 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_en

Case Google – Right to be forgotten

Retrieved 14/05/2018 https://www.theguardian.com/technology/2018/feb/27/right-to-be-forgotten-claimant-wants-to-rewrite-history-says-google

Retrieved 14/05/2018 https://www.theguardian.com/technology/2018/mar/12/right-to-be-forgotten-high-court-hears-second-google-case

Retrieved 14/05/2018 https://www.theguardian.com/technology/2018/apr/13/google-loses-right-to-be-forgotten-case

Retrieved 14/05/2018 https://www.judiciary.gov.uk/wp-content/uploads/2018/04/nt1-nt2-v-google-press-summary-180413.pdf

Case Facebook – Cambridge Analytica

Retrieved 14/05/2018 http://www.bbc.com/news/technology-43465968

Retrieved 14/05/2018 https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought

Case Yahoo

Retrieved 14/05/2018 https://www.theverge.com/2018/4/24/17275994/yahoo-sec-fine-2014-data-breach-35-million

Retrieved 14/05/2018 https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html

Retrieved 14/05/2018 https://www.reuters.com/article/us-altaba-cyber-yahoo/u-s-regulator-fines-altaba-35-million-over-2014-yahoo-email-hack-idUSKBN1HV295

CNIL PIA software

Retrieved 03/06/2018 https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

12 Overzicht van de bijlagen

1. Categorieën van persoonsgegevens
2. Categorieën van ontvangers
3. Schema rapporteren inbreuken betreffende persoonsgegevens
4. Voorbeeld register van verwerkingsactiviteiten
5. Voorbeeld van een balancing test
6. Voorbeeld van een DPIA
7. Landen op de witte lijst voor adequate gegevensbescherming
8. Change Request Approval form
9. Blog – GDPR checklist – part 1 – Communication & Awareness
10. Blog – GDPR checklist – part 2 – (Re)gain control of your business landscape
11. Blog – Interview with the Belgian State Secretary for Privacy Philippe De Backer
12. Blog – GDPR checklist – part 3 – IT governance and control procedures

Bijlage 1: Categorieën van persoonsgegevens

Categorieën van persoonsgegevens die bij de GDPR onder de vorm bijzondere categorieën vallen zijn gemarkeerd in het vet.[7]

- Identificatiegegevens
- Financiële bijzonderheden
- Persoonlijke kenmerken
- Fysieke gegevens
- Leefgewoonten
- **Psychische gegevens**
- Samenstelling van het gezin
- Vrijetijdsbesteding en interesses
- Lidmaatschappen
- Gerechtelijke gegevens
- Consumptiegewoonten
- Woningkenmerken
- **Gegevens betreffende de gezondheid**
- Opleiding en vorming
- Beroep en betrekking
- Rijksregisternummer of Identificatienummer van de sociale zekerheid
- **Raciale of etnische gegevens**
- **Gegevens over het seksuele leven**
- **Politieke opvattingen**
- **Lidmaatschap van een vakvereniging**
- **Filosofische of religieuze overtuigingen**
- Beeldopnamen
- **Genetische gegevens**
- **Biometrische gegevens**
- Locatiegegevens

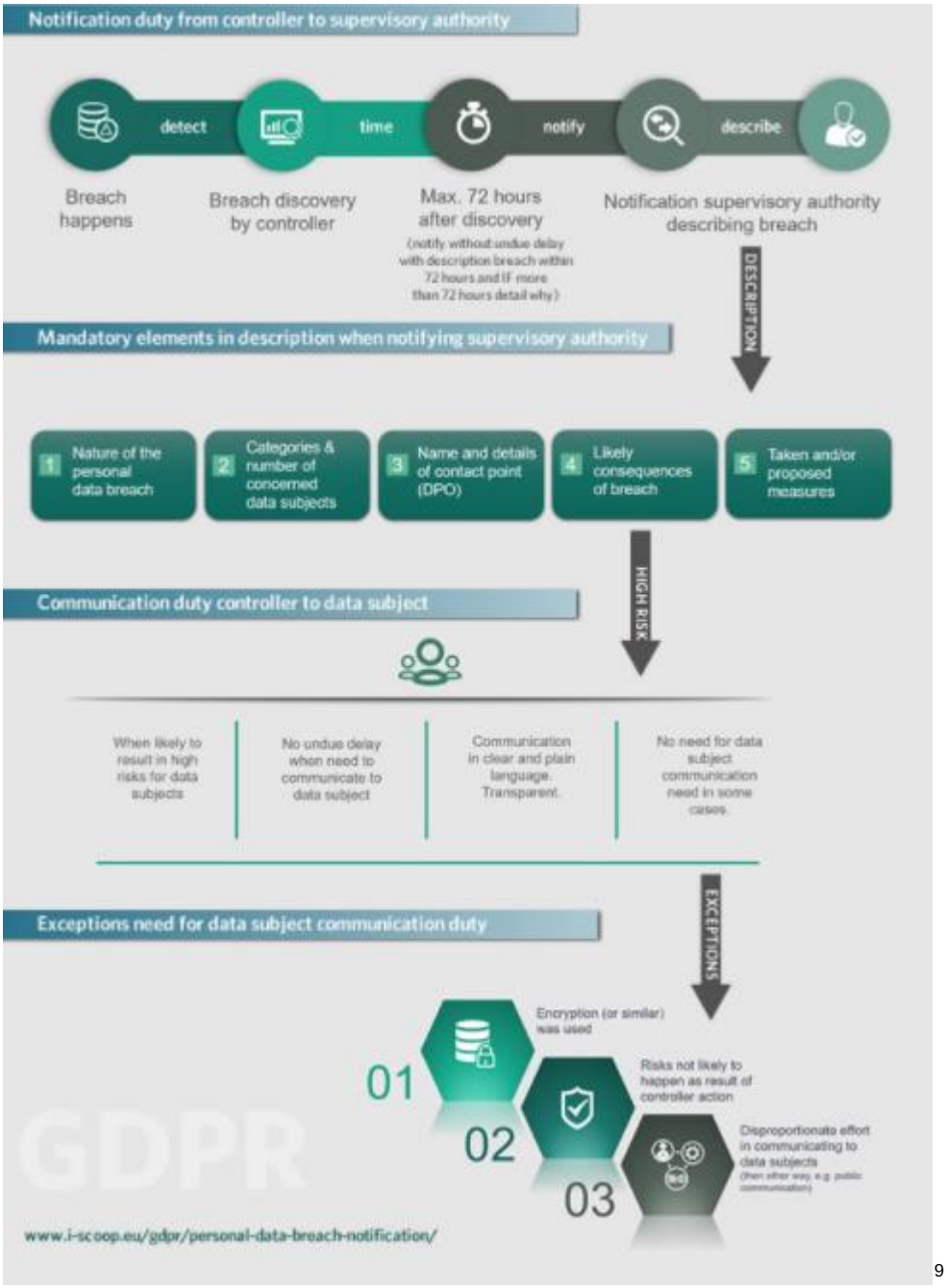
[7]Bron:*https://eloket.privacycommission.be/elg/help/NL/submit_declaration/coding_declarations/categories_data.html*

Bijlage 2: Categorieën van ontvangers[8]

- De geregistreerde persoon zelf
- Persoonlijke relaties van de geregistreerde persoon
- Professionele raadgevers van de geregistreerde persoon
- Werkgever of zakenrelaties van de geregistreerde persoon
- Individuen of organisaties in directe relatie met de verantwoordelijke
- Andere diensten of nevenondernemingen van de verantwoordelijke
- Andere privéondernemingen
- Overheidsdiensten
- Gerecht en politiediensten
- Sociale zekerheidsinstanties
- Banken en verzekeringsmaatschappijen
- Makelaars in persoonsgegevens of direct marketing
- Andere

[8] Bron: *https://whitewire.be/templates/*

Bijlage 3: Schema rapporteren van inbreuken betreffende persoonsgegevens



[9]

[9] Bron: *https://www.i-scoop.eu/gdpr/personal-data-breach-notification/*

Bijlage 4: Voorbeeld register van verwerkingsactiviteiten

Disclaimer: Dit is slechts een voorbeeld en kan niet aan de realiteit van Kinepolis Group NV getoetst worden. Dit is bijgevoegd als meerwaarde om toch visueel een register van verwerkingsactiviteiten te kunnen tonen.

Naam businessproces	Eigenaar proces	Functionele omschrijving verwerking	Nummer	Verwerking	Doel verwerking
Vermeld de naam/beschrijving van het businessproces	Identificeer de eigenaar(s) (functie) van het business proces waartoe de verwerking behoort	Identificatie en informatie over de verwerking *nummer, functionele omschrijving, finaliteit, verwerkingsgrond, type verwerking en functionele beschrijving*	Vul het interne identificatienummer van de verwerking toe	Vermeld de naam/functionele omschrijving van de verwerking	Vermeld het doeleinde van de verwerking in het tabblad 'lijsten' is een indicatieve lijst (indicatieve lijst met type doeleinden) met enkele standaarddoelstellingen opgenomen. Let op: deze lijst dekt evenwel niet alle situaties. De Gegevensbeschermingsautoriteit kan bijvoorbeeld van oordeel zijn dat er voor een welbepaalde verwerking meer precieze informatie vereist is.
Access control	<Confidential>	Human Resources	1	Access Control	Beveiliging
Internal Communication	<Confidential	Internal Communication	2	Interne communicatie	Ander doeleinde
Customer relation management	<Confidential>	CRM	3	Klachtenbehandeling	Klantenbeheer
Customer relation management	<Confidential>	CRM	4	Uitsturen nieuwsbrief	Klantenbeheer
Loyalty kaarten	<Confidential>	CRM	5	Beheer van klanten kaarten	Klantenbeheer

Doel verwerking specifieke omschrijving	Verwerkingsgrond	Verwerkingsgrond extra info	Type verwerking*
Indien er meerdere doelen zijn voor dezelfde verwerking, gebruik dan meerdere lijnen, want elk doel heeft exact 1 verwerkingsgrond. Een doel moet specifiek geformuleerd zijn.	Geef aan wat de verwerkingsgrond voor de verwerking is. In het tabblad 'lijsten' is een overzicht opgenomen van de verschillende mogelijke verwerkingsgronden, zoals vermeld in art.6 AVG. Verduidelijk indien nodig (bv. indien verwerkingsgrond wetgeving is, vermeld de wetgeving).	Vermeld vooral of er in geval van gerechtvaardigde belangen een specifieke legitimate interest assessment werd uitgevoerd	Geef aan om welk type verwerking het gaat: vermeld de voor de verwerking van toepassing zijnde types (zie de lijst 'type verwerking' in het tabblad 'lijsten') vul in 'normaal' als het niet om een type verwerking gaat zoals vermeld in de lijst 'type verwerking' (zie tabblad 'lijsten').
Toegang verlenen aan werknemers	Noodzakelijk voor uitvoering van een overeenkomst	Badgen is nodig om het gebouw binnen te komen, anders kan het arbeidscontract niet uitgevoerd worden	Normaal--> als geen van onderstaande types
Business informatie wordt verspreid op een intern sociaal mediaplatform dat complementair is aan het intranet	Toestemming betrokkene	Het vrijblijvend sociaal medium voor corporate communication	Normaal--> als geen van onderstaande types
Business proces om de klachten en vragen van klanten te behandelen	Noodzakelijk voor uitvoering van een overeenkomst		Normaal--> als geen van onderstaande types
Direct marketing	Gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde	Zie elders	Evaluatie of beoordeling van mensen waaronder profilering en het maken van prognoses
Beheer klantenkaarten	Noodzakelijk voor uitvoering van een overeenkomst	Klantenkaarten staan op naam omdat deze strikt persoonlijk zijn (zoals abonnementen of een studentenkaart)	Normaal--> als geen van onderstaande types

Gebruikte gegevens en betrokkenen Details over de gegevens die verwerkt worden en de betrokkenen van wie gegevens verwerkt worden *functionele categorie, gevoelige categorie gegevensverwerking, categorie betrokken, classificatieniveau, bewaartermijn, authentieke bron*	**Functionele gegevenscategorie** Vermeld de functionele gegevenscategorie(ën) in het tabblad 'lijsten' is een indicatieve lijst ('indicatieve lijst met functionele gegevenscategorieën') met enkele standaarddoelstellingen opgenomen. Let op: deze lijst dekt evenwel niet alle situaties. De Gegevensbeschermingsautoriteit kan bijvoorbeeld van oordeel zijn dat er voor een welbepaalde verwerking meer precieze informatie vereist is.	**AVG-gegevenscategorie*** Geef aan of er gegevenscategorieën verwerkt worden waaraan er bijzondere aandacht moet besteed worden ja --> indien een van de in de lijst 'AVG-gegevenscategorie' (zie tabblad 'lijsten') gegevenscategorieën verwerkt wordt nee --> indien het niet om een categorie gaat zoals vermeld in de lijst 'AVG-gegevenscategorie' (zie tabblad 'lijsten').	**Verwerkingsgrond sensitieve gegevens**	**Categorie(en) betrokkenen** Vermeld de categorie(ën) van betrokkenen
Naam, familienaam, duim	Identificatiegegevens	Biometrische gegevens met het oog op de unieke identificatie van een persoon	Noodzakelijk voor arbeids-, socialezekerheidswet-, socialebeschermingsrecht	Medewerkers
Contactgegevens en publicaties op tijdslijn	Persoonlijke identificatiegegevens	Geen sensitieve gegevens	Geen sensitieve gegevens	Medewerkers
Contactgegevens, vragen en klachten van de klant	Identificatiegegevens en vrij invulveld	Geen sensitieve gegevens	Geen sensitieve gegevens	Klanten
Contactgegevens, interesses	Persoonlijke kenmerken	Geen sensitieve gegevens	Geen sensitieve gegevens	Klanten
Contactgegevens, interesses, foto	Persoonlijke kenmerken	Biometrische gegevens met het oog op de unieke identificatie van een persoon	Noodzakelijk voor rechtsvordering of voor gerechten	Klanten

Kwetsbare categorie betrokkenen*	Bewaartermijn	Koppeling gegevens	Authentieke bron	Verwerker	Naam	nr. gegevensverwerkings-contract
Geef aan of de betrokkenen tot een kwetsbare categorie behoren ja --> indien het betrokkenen betreft die zich in een situatie bevinden waarin een onevenwicht in de relatie tussen de positie van een betrokkene en een verwerkingsverantwoordelijke is, zoals bijvoorbeeld kinderen, werknemers, patiënten, ... nee --> indien het niet om een categorie betrokkenen zoals hierboven vermeld	Geef aan wat de bewaartermijn van de verwerkte gegevens is	Geef aan of er gegevens uit verschillende datasets worden gekoppeld.	Vermeld de bron van gegevens indien deze niet de betrokkene zelf is	Identificatie van de verwerker (extern aan organisatie) die betrokken is bij de verwerking *naam, nr. gegevensverwerkingscontract*	Vul de naam van de verwerking in. Indien gekend, een officieel identificatienummer tussen haken	Vul het nummer/titel van het (de) gegevensverwerkingscontract(en) in
Ja	<Confidential>	N/a	Eigen verwerking			
Ja	<Confidential>	N/a	Eigen verwerking			
Geen	<Confidential>	N/a	Eigen verwerking			
Geen	<Confidential>	N/a	Eigen verwerking			
Geen	<Confidential>		Eigen verwerking			

Gegevensuitwisseling	Categorie(ën) gegevens	Categorie(ën) ontvangers	Derde land/internationale organisatie	Aard van de doorgifte naar een derde land/internationale organisatie
Informatie over eventuele gegevensuitwisseling met derde partijen categorie(ën) gegevens, *categorie(ën) ontvangers, derde land/internationale organisatie, documenten passende waarborgen*	In voorkomend geval, vermeld de categori(ën) van gegevens die uitgewisseld worden	In voorkomend geval, geef aan welke de categorie(ën) van ontvangers is (zijn). In het tabblad 'lijsten' is een indicatieve lijst ('categorie(ën) ontvangers') met enkele standaarddoelstellingen opgenomen. Let op: deze lijst dekt evenwel niet alle situaties. De Gegevensbeschermingsautoriteit kan bijvoorbeeld van oordeel zijn dat er voor een welbepaalde verwerking meer precieze informatie vereist is.	In voorkomend geval, vermeld de derde landen/internationale organisaties bij doorgifte van persoonsgegevens definitie "derde land": alle landen buiten de Europese Unie (EU) en de Europese Economische ruimte (EER) definitie "internationale organisatie": een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen	In voorkomend geval, vermeld de aard van de doorgifte naar de derde landen/internationale organisaties In het tabblad 'lijsten' is een overzicht opgenomen van de verschillende mogelijkheden
			Geen	Niet van toepassing
			Geen	Niet van toepassing
			Geen	Niet van toepassing
			Geen	Niet van toepassing
			Geen	Niet van toepassing

Documenten passende waarborgen Indien doorgifte persoonsgegevens naar derde land/internationale organisatie + doorgifte op basisvoorwaarde art. 49.2 AVG vermeld de documenten die de genomen passende waarborgen verduidelijken en waar deze terug te vinden zijn	**Technologie** Beschrijving van de gebruikte technologie, applicaties, software bij de verwerking	**Beschrijving** Vermeld op welke wijze deze verwerking wordt uitgevoerd welke technologie (bv. Cloud based, block chain, …), applicatie of software wordt hiervoor gebruikt?	**Risico & beveiligingsmaatregelen** Informatie over het risico en de beveiligingsmaatregelen van de gegevensverwerking *risico, beschrijving beveiligingsmaatregelen, documentatie beveiligingsmaatregelen, GEB (DPIA)*	**Risico** Geef het inherente risico voor de fundamentele rechten en vrijheden van de betrokkenen aan.	**Beschrijving beveiligingsmaatregelen** Geef in algemene bewoording de voor de specifiek voor de verwerking genomen technische en organisatorische beveiligingsmaatregelen technische en organisatorische beveiligingsmaatregelen op business niveau moeten niet an sich vermeld worden. Vermeld hiervoor "standaard maatregelen"
	Database	Database	Zie elders	Zie elders	Zie elders
	Webapplicatie en mobile applicatie	Webapplicatie en mobile applicatie	Zie elders	Zie elders	Zie elders
	Website met invulformulieren	Webapplicatie die invulformulieren heeft gekoppeld aan een mailadres voor de klachtenbehandeling	Zie elders	Zie elders	Zie elders
	Webapplicatie en mobile applicatie gekoppeld aan CRM-systeem	<Confidential>	Zie elders	Zie elders	Zie elders
	Web portaal met database	<Confidential>	Zie elders	Zie elders	Zie elders

Documentatie Verwijzing naar de documenten met de beschrijving van de "standaard maatregelen" en de specifiek voor de verwerking genomen technische en organisatorische beveiligingsmaatregelen	**Resultaat GEB (DPIA)** Indien de verwerking een waarschijnlijk hoog risico inhoudt voor de fundamentele rechten en vrijheden van de betrokkenen, moet een GEB uitgevoerd worden (art.135 AVG) vermeld het resultaat van de GEB, alsook een referentie naar het document dat de GEB bevat	**Rechten betrokkenen** Verwijzing naar de documenten die de procedures ter respectering van de rechten van de betrokkenen bepalen	**Informeren betrokkenen** Geef aan hoe de betrokkenen in kennis worden gesteld van de registratie van hun gegevens	**Procedure uitoefening rechten** Geef aan welk document deze procedure beschrijft geef aan welke, in voorkomend geval, de voor deze verwerking bijzondere maatregelen voor de uitoefening van de rechten van de betrokkenen zijn	**Status** Informatie over de status van de verwerking: startdatum, einddatum en plaatsvervangende verwerking
Zie elders	Niet van toepassing		Contract bij afhalen badge		
Zie elders	Niet van toepassing		Arbeidscontract	Uitoefening rechten gebeurd bij Communication Manager	
Zie elders	Zie elders		Versturen formulier	Instellingen van account of DPO contacteren	
Zie elders	Zie elders		Aanmaak account	Instellingen van account	
Zie elders	Zie elders		Bij registreren	Selfservice portaal	

Startdatum verwerking	Einddatum verwerking	Plaatsvervangende verwerking	Datum laatste update
Startdatum verwerking	Indien van toepassing, einddatum verwerking. Deze datum invullen houdt in dat de verwerking niet langer uitgevoerd wordt. Doorstreep dan ook direct de volledige lijn.	Vermeld, in voorkomend geval, het nummer van de verwerking die de stopgezette verwerking vervangt. Dit zorgt voor een historiek in het register Dit kan nuttig zijn wanneer bijvoorbeeld de verwerkingsgrond zou wijzigen door bijvoorbeeld een wetswijziging.	Datum laatste update van de informatie m.b.t. deze gegevensverwerking in dit register

<Confidential>	<Confidential>		
<Confidential>	<Confidential>		
<Confidential>	<Confidential>		
<Confidential>	<Confidential>		
<Confidential>	<Confidential>		

Bijlage 5: Voorbeeld van een balancing test

Disclaimer: Dit is slechts een voorbeeld en kan niet aan de realiteit van Kinepolis Group NV getoetst worden. Dit is bijgevoegd als meerwaarde om toch visueel een balancing test te kunnen tonen.

Asset	Marketinglijst		
Processing activity	Uitsturen van newsletters		
Question	**Answer**	**Extra explanation**	**Guidance**
Identifying a legitimate interest			
What is the purpose of the processing operation?	Het uitsturen van newsletters.	Klanten een newsletter sturen met een update over nieuwe content.	The first stage is to identify to a Legitimate Interest – what is the purpose for processing the personal data?
Is the processing necessary to meet one or more specific organisational objectives?	Ja.	De mails worden uitgestuurd in het belang van de onderneming en om klanten op de hoogte te brengen van updates.	If the processing operation is required to achieve a lawful business objective, then it is likely to be legitimate for the purposes of this assessment.
Is the processing necessary to meet one or more specific objectives of any Third Party?	Nee.	Voor deze verwerking gebruiken we geen derde partijen.	While you may only need to identify one Legitimate Interest for the purposes of an LIA – the interest that you are seeking to rely on - it may be useful to list all apparent interests in the processing, those of you as the Controller, as well as those of any Third Party who are likely to have a Legitimate Interest.
Does the GDPR, ePrivacy Regulation or other national legislation specifically identify the processing activity as being a legitimate activity, subject to the completion of a balancing test and positive outcome?	Ja.	Direct marketing wordt gezien als een legitiem belang van de onderneming.	For example: Legitimate Interests might be relied on where an individual's (including client or employee) information is processed by a group of companies for the purposes of administration (Recital 48). If the Controller is processing sensitive Personal Data in the employee context, then they may be able to rely on Article 9(2) (b).

Is the interest lawful?	Ja.		in accordance with EU and national law
is the interest sufficiently concrete?	Ja.	De verwerking is nodig voor het uitvoeren van een legitiem belang van de onderneming, en is voldoende geconcretiseerd.	sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject
is the interest not speculative?	Neen.	Het belang van de onderneming is voldoende duidelijk.	represent a real and present interest
The necessity test			
Why is the processing activity important to the Controller?	De contactgegevens van klanten zijn nodig voor het uitsturen van deze newsletters. Daarnaast is direct marketing een belangrijk bedrijfsproces voor het onderhouden van klantenrelaties.		A Legitimate Interest may be elective or business critical; however, even if the Controller's interest in processing personal data for a specific purpose is obvious and legitimate, based on the objectives of the Controller, it must be a clearly articulated and communicated to the individual.

Why is the processing activity important to other parties the data may be disclosed to, if applicable?	Niet van toepassing		A Legitimate Interest could be trivial or business critical, however, the organization needs to be able to clearly explain what it is. Some purposes will be compelling and lend greater weight to the positive side of the balance, while others may be ancillary and may have less weight in a balancing test. Consider whether your interests relate to a fundamental right, a public interest or another type of interest. Just because the processing is central to what the organization does, does not make it legitimate. It is the reason for the processing balanced against the potential impact on an individual's rights that is key. It is important to consider whose Legitimate Interests are being relied on. Understanding this will help inform the context of the processing. In combination with the reason the Personal Data is being processed, this information will determine the weight of the Legitimate Interest that needs to be balanced.

Is there another way of achieving the objective?	Neen.		• If there isn't, then clearly the processing is necessary; or • If there is another way but it would require disproportionate effort, then the processing is still necessary; or • If there are multiple ways of achieving the objective, then a Privacy Impact Assessment should have identified the least intrusive means of processing the data which would be necessary; or • If the processing is not necessary (It is unlikely that there will be many scenarios where a processing operation is not necessary where it has been identified as being a means to achieve a stated business objective), then Legitimate Interests cannot be relied on as a lawful basis for that processing activity
The balancing test (including references to mitigation measures)			
Would the individual expect the processing activity to take place?	Ja de betrokken persoon kan zelf kiezen of hij deze mails ontvangt of niet.		If individuals would expect the processing to take place then the impact on the individual is likely to have already considered by them and accepted. If they have no expectation, then the impact is greater and is given more weight in the balancing test
Does the processing add value to a product or service that the individual uses?	Ja, hij wordt op de hoogste gesteld van nieuwe content waar hij eerder al interesse in toonde.		
Is the processing likely to negatively impact the individual's rights?	Neen, de betrokken persoon kan op elk moment het ontvangen van deze mails afzetten.		

Is the processing likely to result in unwarranted harm or distress to the Individual?	Neen, er wordt geen gebruik gemaakt van sensitieve gegevens of gegevens die schaden kunnen brengen.		
Would there be a prejudice to Data Controller if processing does not happen?	Ja, hierdoor kan de verwerkingsverantwoordelijk contact nemen met klanten en hen op de hoogte houden.		
Would there be a prejudice to the Third Party if processing does not happen?	Niet van toepassing		
Is the processing in the interests of the individual whose personal data it relates to?	Ja, op deze manier krijgt hij informatie over eigen interesses die hij eerder vertoonde.		
Are the legitimate interests of the individual aligned with the party looking to rely on their legitimate interests for the processing?	De verwerking is in het voordeel van beide partijen.		What are the benefits to the individual or society? If the processing is to the benefit of the individual, then it is more likely that Legitimate Interests can be relied on, as the individual's interests will be aligned with those of the Controller. Where the processing is more closely aligned with the interests of the Controller or a Third Party, than with those of the individual, it is less likely that the interests will be balanced and greater emphasis needs to be placed on the context of the processing and relationship with the individual.
What is the connection between the individual and the organization?	De betrokken persoon is een klant.		

What is the nature of the data to be processed? Does data of this nature have any special protections under GDPR?	Er wordt enkel gebruik gemaakt van contactgegevens en eerder vertoonde interesses.		Data relating to a child etc. If processing Special Categories of Personal Data, an Article 9 condition must be identified as the lawful basis of processing.
Is there a two-way relationship in place between the organization and the individual whose personal information is going to be processed? If so how close is that relationship?	De verwerking is in het kader van een klantenrelatie, dus ja er is een tweezijdige relatie.		Where there is an ongoing relationship, or indeed a more formal relationship, there may well be a greater expectation on the part of the individual that their information will be processed by the organization. The opposite is also possible but it does depend on the purpose of processing.
Would the processing limit or undermine the rights of individuals?	Neen.		If processing would undermine or frustrate the ability to exercise those rights in future that might well affect the balance.
Has the personal information been obtained directly from the individual, or obtained indirectly?	Ja de betrokken persoon kan zelf kiezen of hij deze mails ontvangt of niet. En heeft zelf de gegevens verstrekt.		If the information was obtained directly from the individual then you should take due consideration of the notice of fair processing (e.g. your Privacy Notice), the relationship with the individual and their expectations of use. If the data was collected directly and these factors are positive, then it may help to tip the balance in favor of the processing operation. Where Personal Data is not collected directly, there may need to be a more compelling Legitimate Interest to overcome this. It will also depend on the context of the processing and if the organization has a two-way relationship with the individual.

Is there any imbalance in who holds the power between the organization and the individual?	Neen er is geen sprake van een gezagsrelatie.		Does the individual have a choice regarding the processing of their personal information? If the organization has a dominant position, this will tip the balance slightly against the use of Legitimate Interests. That said, the rights and freedoms of individuals laid down in the GDPR go some way to redressing this issue. The Controller will need to consider how it addresses any imbalance of power to ensure individuals' rights are not impacted.
Is it likely that the individual may expect their information to be used for this purpose?	Ja de persoon gaf zelf zijn gegevens op, schreef zelf in op de mailinglist en werd op de hoogte gesteld hoe de gegevens verwerkt werden.		Given the relationship between the parties, services/products being provided, including the information notices available, would the individual reasonably expect or anticipate that their information would be used for those or connected purposes? The stronger the expectation, the greater the chances that Legitimate Interests can be relied on.
Could the processing be considered intrusive or inappropriate? Could it be perceived as such by the individual or in the context of the relationship?	Neen, de persoon werd op de hoogte gesteld hoe gegevens verwerkt worden, en kan bovendien ook uitschrijven indien gewenst.		Processing should not be unwarranted - intrusion into the private life of an individual may be justified based on the nature of the relationship or special circumstances. However, the greater the intrusion, perceived or otherwise, the more overwhelming the Legitimate Interest should be and the more the rights of the individual must be considered within the balance. Consider here the way the data is processed (e.g. large scale, data mining, profiling, disclosure to many people or publication).

Is a fair processing notice provided to the individual, if so, how? Are they sufficiently clear and up front regarding the purposes of the processing?	Ja, er wordt een link gelegd naar het privacy statement waar de uitleg over de verwerking kan gevonden worden.		Remember that the more unusual, unexpected or intrusive the processing, the greater the importance of making the individual aware of the processing. Particularly where Legitimate Interests are to be relied on.
Can the individual, whose data is being processed, control the processing activity or object to it easily?	Ja, hij kan op ieder welk moment van de verwerking uitschrijven.		Giving the individual increased control or elements of control may help a Controller rely on Legitimate Interests where otherwise they could not. If individual control is not possible or not appropriate, explain why.
Can the scope of the processing be modified to reduce/mitigate any underlying privacy risks or harms?	De gebruikte gegevens worden reeds beperkt tot een minimum.		This is a similar concept to a Data Protection Impact Assessment. Where a DPIA might identify potential privacy harms it also allows the organization to mitigate the risk of non-compliance by adapting or altering the scope of the activity. The same is true for an LIA. If you conclude that the processing presents a privacy risk to the individual, the processing can be limited or adapted to reduce the potential impact.
Safeguards and compensating controls			
Logical access control	Enkel gemachtigde personen mogen dergelijke mails uitsturen.		
Assessment of accountability, transparency, right to object and beyond			
The existence of some and possible need for additional measures to increase transparency and accountability;			

The right of the data subject to object to the processing, and beyond objection, the availability of opt-out without the need for any justification;	Ja	Uitschrijven kan op elk moment via de link onderaan in de email.	
Empowering data subjects: data portability and the availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data.	Ja	Dit wordt beschreven in het privacy statement.	
Reaching a decision and documenting the outcome			
Outcome of the assessment	[Balanced/Unbalanced]		
Signed by	[Data Protection Responsible Name]		
Role	[Data Protection Responsible Role]		
Date	[Date]		
Next review date	[Date]		
Communication of this assessment to data subjects (transparency and visibility)	[Yes/No]		

Bijlage 6: Voorbeeld van een DPIA

Disclaimer: Dit is slechts een voorbeeld en kan niet aan de realiteit van Kinepolis Group NV getoetst worden. Dit is bijgevoegd als meerwaarde om toch visueel een data prrocessing impact assessment te kunnen tonen. Merk ook op dat in werkelijkheid de auteur, assessor en validator verschillend zijn om een "conflict of power/interest" te vermijden.

PIA information

PIA
Biometrics for fingerprinting

Author's name
Kevin,Bollengier

Assessor's name
Kevin,Bollengier

Validator's name
Kevin,Bollengier

Creation date
03/06/2018

DPO's name
Kevin Bollengier

DPO's opinion
This is a secure way to work with biometric data.

Search of concerned people opinion
Concerned people opinion was requested.

Concerned people opinions
HR Management

Concerned people statuses
The treatment could be implemented.

Concerned people opinions
Needs verification with the employees.

Context

Overview

Which is the processing under consideration?

Fingerprint badging sytem for time registration, used against fraud.

What are the responsibilities linked to the processing?

The processor needs to store the fingerprints in a hashed format using a fuzzy vault algorithm which is a nowadays standard.

Are there standards applicable to the processing?

There needs to be a secure algorithm to hash the fingerprints.

Evaluation : Acceptable
Evaluation comment :
This is a safe and secure way to store fingerprints.

Data, processes and supporting assets

What are the data processed?

Employee names linked to a hashed fingerprint.

How does the life cycle of data and processes work?

When an employee starts working he chooses between a fingerprint or badge system to clock in his work hours. When an employee leaves the company, the data is removed.

What are the data supporting assets?

We use a dedicated software with a database connected which is running on the badge device.

Evaluation : Acceptable

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

The processing is in our legitimate interest as using a fingerprint is the only optimal method for fraud detection.

Evaluation : Acceptable
Evaluation comment :
This is indeed a necessary process to verify if employees were fraudulent or not.

What are the legal basis making the processing lawful?

Explicit consent

Evaluation : Acceptable
Evaluation comment :
Explicit consent.

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

Yes the use of fingerprints is the only method where we can detect fraud.

Evaluation : Acceptable

Are the data accurate and kept up to date?

Yes.

Evaluation : Acceptable

What are the storage duration of the data?

The duration of the employee's contract.

Evaluation : Acceptable

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

On the administrative welcome they receive all required information to perform their work duties.

Evaluation : Acceptable

If applicable, how is the consent of data subjects obtained?

The employees receive a consent form where they can indicate their choice between the fingerprint or badge system.

Evaluation : Acceptable

How can data subjects exercise their rights of access and to data portability?

With the HR manager.

Evaluation : Acceptable

How can data subjects exercise their rights to rectification and erasure?

The data can only be erased when switching to a physical badge system or when the contract ends.

Evaluation : Acceptable

How can data subjects exercise their rights to restriction and to object?

With the HR manager, although the fingerprint will be replaced with a physical badge as the clocking hours are required for the employee administration regarding salaries.

Evaluation : Acceptable

Are the obligations of the processors clearly identified and governed by a contract?

Yes, the processor we use signed a data processing agreement.

Evaluation : Acceptable

In the case of data transfer outside the European Union, are the data adequately protected?

Not applicable, we store the data in our own network.

Evaluation : Acceptable

Risks

Planned or existing measures

Fuzzy vault hashing algorithm

We use a fuzzy vault hashing algorithm to ensure the confidentiality and integrity of the employee's biometric data.

Evaluation : Acceptable
Evaluation comment :
Backups

Encrypted back-ups

We have encrypted back-ups stored in a physical different location to ensure business continuity.

Evaluation : Acceptable

Duplicated datacenter

We have a duplicated hot swappable datacenter in place to ensure business continuity.

Evaluation : Acceptable

Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?
No accurate payment of salaries
What are the main threats that could lead to the risk?
Unavailability of the system.
What are the risk sources?
Power cut, Fire
Which of the identified controls contribute to addressing the risk?
Fuzzy vault hashing algorithm
How do you estimate the risk severity, especially according to potential impacts and planned controls?
Limited, A paper form could be used when the badging system is down. Therefore salaries will still be able to be paid accurately, although there is more administrative work.
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?
Negligible, The risks are negligible to occur.

Evaluation : Acceptable

Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?
No accurate payment of salaries
What are the main threats that could lead to the risk?
Human error, Malicious intent
What are the risk sources?

Human sources

Which of the identified controls contribute to addressing the risk?

Fuzzy vault hashing algorithm

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Negligible, Modification of the database is strictly limited to application administrators

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, Modification of the database is strictly limited to application administrators.

Evaluation : Acceptable

Data disappearance

What could be the main impacts on the data subjects if the risk were to occur?

No accurate payment of salaries.

What are the main threats that could lead to the risk?

Network downage, Broken badge scanner, Human error

What are the risk sources?

Malicious intent (Revenge), Human error, No scalability

Which of the identified controls contribute to addressing the risk?

Encrypted back-ups, Duplicated datacenter

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Negligible, The risks are limited as we have back-ups.

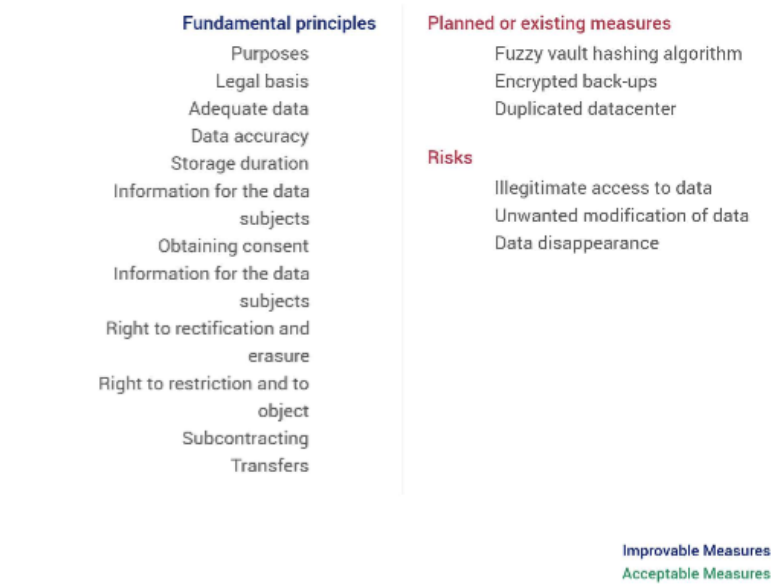
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible, So far we never experienced problems with the badge scanners.

Evaluation : Acceptable

Action plan

Overview



Fundamental principles

No action plan recorded.

Existing or planned measures

No action plan recorded.

Risks

No action plan recorded.

Risks overview

Potential impacts

- No accurate payment of sala...
- No accurate payment of sala...

Threats

- Unavailability of the system.
- Human error
- Malicious intent
- Network downage
- Broken badge scanner

Sources

- Power cut
- Fire
- Human sources
- Malicious intent (Revenge)
- Human error
- No scalability

Measures

- Fuzzy vault hashing algorithm
- Encrypted back-ups
- Duplicated datacenter

Illegitimate access to data

Severity : Limited

Likelihood : Negligible

Unwanted modification of data

Severity : Negligible

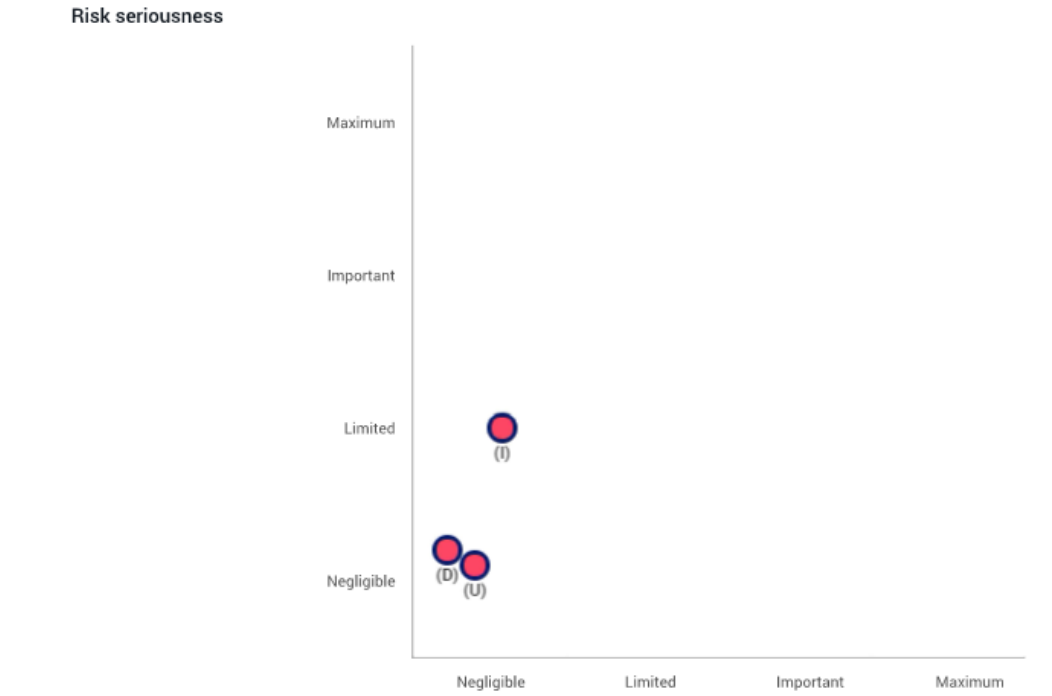
Likelihood : Negligible

Data disappearance

Severity : Negligible

Likelihood : Negligible

Risk mapping



- Planned or existing measures
- With the corrective measures implemented
- (I)llegitimate access to data
- (U)nwanted modification of data
- (D)ata disappearance

03/06/2018

[10] Software: CNIL Privacy Impact Assessment tool

Bijlage 7: Landen op de witte lijst voor adequate gegevensbescherming

Volgende landen zijn op moment van schrijven erkend voor het aanbieden van een adequate gegevensbescherming:[11]

- Andorra
- Argentinië
- Canada (Commerciële organisaties)
- Faeröer eilandengroep
- Guernsey
- Israël
- Eiland Man
- Jersey
- Nieuw-Zeeland
- Zwitserland
- Uruguay
- US (Privacy Shield framework)

[11] Bron: *https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en*

Bijlage 8: Change Request Approval form

Request Title/Name	
Request department	
Project Manager	
Creation Date (dd/mm/yyyy)	
Requested Deployment Date (dd/mm/yyyy)	

Change Deployment Info	
Fill in with appropriate information	
Software/module to change: _____	
Details of change	
Reason for change	
Business impact	
Rollback scenario	
Planned maintenance Action check	
Date Planned Maintenace Communication	

I have reviewed the information contained in this Change/Work request form and approve of this change. The change can only be implemented when all of the following signatures are present:

Data Protection Officer	Project Manager
Technical Owner	Application owner
IT Security & Compliance Officer	Business Intelligence
CIO	

GDPR CHECKLIST – PART 1 – COMMUNICATION & AWARENESS

March 7, 2018 in GDPR and Business by Kevin Bollengier 0 Comments

In this blogging series I will try to hand you quick, easy and fairly cheap methods to help achieve one of the goals of GDPR namely security and privacy by default.

WHAT IS SECURITY AND PRIVACY BY DESIGN/DEFAULT?

Security and privacy by design is one of the key principles of the new regulation as seen in article 25.

Privacy and security by design requires a company to process personal data with data protection and security in mind in every step.

These steps include the design process, development, design of the IT infrastructure and much more. In short it means that privacy and security must be built-in for the entire lifecycle of the process.

THE IMPORTANCE OF COMMUNICATION AND AWARENESS

It will be the **duty of the Data Protection Officer (DPO)** to maintain compliance to the new regulation. However every single employee will have the responsibility to handle personal data with care. And often people working with personal data have not been made aware of GDPR. They might have heard that there is a large "GDPR-project" running and that is a lot of work etc. However they might not know the big changes that will come with the new regulation. As company you will be the one liable for possible data breaches. So having your employees informed is in your best interest.

ATTITUDE CHANGE

GDPR requires a change in attitude of handling personal data and this will have its impact on your business processes. As a company you want a clear vision on how your company functions. But most of all, you want your company to be compliant to GDPR. This can be a difficult process especially in older companies which have the attitude of a family business. The solution is to have your GDPR team organize training sessions and awareness campaigns.

INVOLVE YOUR EMPLOYEES

Employees like it when you involve them in new projects and inform them about updates or changes regarding to the company. So involve them. Achieve this by sending a clear communication explaining GDPR and the changes it brings. Explain what rights the data subject will benefit and which duties the company has towards the data subject but most of all the importance of GDPR. You can find more on employee rights **here**.

MAINTAIN AWARENESS

Send regular reminders about good practices how your employees should handle personal data with care (e.g. only send copies of files containing personal data if necessary and only send them using official company communication channels). Another option is to have e-learnings within the company using the IT Governance you have installed, which by the way will be another topic in a following blog.

So make sure your company and employees are ready for 25/05/2018!

Bron: https://eugdprcompliant.com/gdpr-checklist-1-communication-awareness/

Of scan volgende QR code:

GDPR CHECKLIST – PART 2 – (RE)GAIN CONTROL OF YOUR BUSINESS LANDSCAPE

March 14, 2018 in GDPR and Business by Kevin Bollengier 0 Comments

THE PROBLEM OF "ROGUE" ASSETS

"Rogue" assets are a problem that fast growing companies often struggle with.

Due to fast expansion of your business, assets like servers, databases and applications… often get forgotten or are added without the correct approval of superiors.

The problem here is that when growing and expanding quickly these assets stay in the dark and often don't receive patches or other employees might not even know they exist.

Due to lack of proper asset management these assets become a vulnerability in your business environment.

MAPPING OUT THE BUSINESS APPLICATIONS

A great way to regain control is to start of from your applications. Applications handle data and often this data will be subject to GDPR.

The following tips are not requested by GDPR directly. But they can be of great help to fill in the register of processing activities as required by article 30 of GDPR.

Start off with building an application inventory, containing the following information:

- Name of the vendor of the application
- Name of the application
- A check if the application contains personal data or not
- The categories of personal data that are processed within the application
- Implemented security measures
- The hosting provider
- The physical location (the country) where the data is processed

In a later stadium you can make a visual model to visualize the flows of data within your business landscape. This will create a very clear view for your business and will help you to locate personal data. This visualization will also help for your internal transparency.

MAPPING OUT THE DATABASE LANDSCAPE

In this exercise will collect all the databases in a similar way.

The following information can be valuable:

- Name of the database server
- Type of database that is running on the server
- Database instances running on the server

This will be used to physically locate data and create an overview which servers require patches. The database instance names can be used to map the applications from the previous exercise with their corresponding databases.

IT GOVERNANCE

To stay in control you will need to create policies. For example a change request policy to make sure that all changes require the signature of the correct superiors and no "rogue applications" enter your infrastructure. A change management policy that requires signatures when the production environment will be changed and that requires the application list, database list and the application and database landscapes to be updated.

This way you will always have a clear view on your internal operations.

To read more on how the GDPR will change the face of business, check out **this article** on our blog.

Bron: https://eugdprcompliant.com/gdpr-checklist-part-2-regain-control-business-landscape/

Of scan volgende QR code:

INTERVIEW WITH THE BELGIAN STATE SECRETARY FOR PRIVACY PHILIPPE DE BACKER

March 21, 2018 in GDPR and Business by Kevin Bollengier 0 Comments

As I'm currently working on my bachelor thesis regarding the impact of GDPR on the IT processes in a multinational business environment, I invited our Belgian State Secretary for privacy for a short interview regarding GDPR. Philippe De Backer accepted and I met him at the Infosecurity conference in Brussels.

Hi Philippe, first of all, thank you very much for doing this in your probably very busy schedule.
No worries, if it's fine I'll just read and answer the questions straight away to save time.

If you had to pick 5 words to describe GDPR, which would you pick?
I think that the GDPR means **standardization**, better **privacy protection** for the **consumer**, a higher level of **compliance** from businesses but most of all an **opportunity** for a business to get a clear view on its data and how they can use that data in the business.

Why do you think GDPR is required?
I think GDPR is absolutely necessary because we are living in a digital economy, an environment where the protection of personal data regarding civilians should be better. The business needs to get a better view which data they have and what they should do with it. But it is also a matter of trust towards clients, GDPR is a framework in which you can say towards your clients "Look we are compliant, you can trust us with your data".

GDPR was established to unite the laws of different Member States of the European Union, yet GDPR allows Member States to fill in some of the gaps of GDPR, isn't this contradictory?
GDPR indeed created a "playing field" for Member States of the European Union, but the gaps they can fill in on a national level are rather limited. The biggest part that will be filled in on national level is the controlling entity, the new Data Protection Authority (DPA). This could be problematic because, this again will lead to fragmentation towards the goal of having a uniformly data protection legislation.

Recently in Datanews there was an interview with Willem Debeuckelaere (Belgian Federal Privacy Commission) that the privacy commission will not be ready on the GDPR deadline, what will be the consequences of this?
Yes this is correct, Willem did say the privacy commission is not ready. I think it's odd that the chairman of the federal privacy commission said this because his only duty is to make sure the federal privacy commission is ready for the GDPR deadline on the 25th of May. In my opinion that wasn't a really smart statement. The privacy commission should push forward, should do more to help companies get compliant, to inform civilians of their newly gained rights and freedoms. This is, in my opinion, the core exercise for the new Data Protection Authority we created.

One of the new aspects of GDPR are the Data Protection Officers, in Spain they need to be certified, can we expect something similar in Belgium?
The DPO certification is not mandatory under GDPR. We also don't have the people or resources to overview this, however this creates a market for universities and colleges which started their own DPO education programs. This is great as I love an open market, but it's also important to have a link with these institutes to ensure the quality of these educations.

GDPR offers a lot of new rights to data subjects, will there be a campaign to the public to create awareness for this?
GDPR indeed opens up a lot of new rights and freedoms towards data subjects. We already worked alongside organizations like VOKA and UNIZO (business federations). Every week the subject of GDPR and data protection makes it in newspapers or magazines. The privacy commission is also working on a roadmap for companies what they need to do. The sector federation Agoria even developed their own tool. So to conclude I think that on all levels we tried to make clear towards the business what needs to happen.

Does a controller require to keep track when for example a user wants to use his "right to be forgotten" as proof?
If a data subject calls upon his "right to be forgotten", you indeed need to be able to show that the rights of the data subject are properly executed. In fact, when the DPA performs an audit, this will be one of the controls. This of course does not mean you need to log the specific details. The evidence that will be required is to show that you have proper, working procedures in place for responding towards the requests of data subjects.

In case there is profiling without legal effects on the data subject (for example movie preferences), is explicit consent required?
Yes, profiling, this is something for which people should always give their explicit consent. In fact a time ago I had a big discussion with the telecom companies Telenet and Proximus. As you might know they perform excessive profiling on the viewing behavior of their clients. I made them very clear that for all new clients they will need to ask explicit consent, this is because under the GDPR everyone benefits of the highest level of privacy and data protection, meaning they have a choice if they want to be subject of profiling to receive movie or advertisement suggestions. This is and remains a consumer choice and is something I stand for.

The new E-privacy legislation was delayed to a later date, what will the impact be on the execution of GDPR in the period that the old E-privacy directive will still be in use?
The E-privacy legislation indeed is linked with GDPR but as such it won't have a direct impact. This is because GDPR is a stand-alone legislation which indeed is of effect as of the 25th of May. Companies will need to be compliant with GDPR as of that deadline, but there are still discussions about the E-privacy legislation, meaning this will be of effect on a later date. It would have indeed been more pleasant if they would be of effect together on the 25th of May, but I don't expect there will be an impact.

According to GDPR, the processing of personal data with a high risk should be reported to the Data Protection Authority. The business can do a Data Protection Impact Assessment to calculate the risk of processing, but what are the standards of the DPA in Belgium?
There were some discussions about this lately as well, also within the Working Party 29, to define what is a high risk and what isn't. I think the Data Protection Authority should provide standards as quickly as possible on how to handle data which is considered as a high risk. But I can guarantee that companies like hospitals are already putting in a great effort to achieve this.

My research for my bachelor thesis is called "What is the impact of GDPR on the IT processes of an international business?".
The first step will obviously be to make sure that the company is compliant in the country where its headquarters is located. The next step is to roll out the changes related to GDPR towards the entire organization. This will in turn require training of the employees on how they should handle, manage and store personal data. Also when we are talking about data transfers outside the European Economic Area, the company will need to make sure they have a legal ground and contract. This is to make sure the game rules of GDPR are followed, not only in a formal and legal way but that they are also implemented practically and operationally. Everything will also need to be logged in the register for audit purposes, to proof compliance and measures taken to protect personal data.

A lot of businesses say that GDPR is an enormous cost to be compliant to the new regulation, what is your opinion on this statement?
GDPR indeed is a compliance cost. But I like to see it more as an opportunity for companies to gain a clear view on the data they possess, to better protect their environments and the personal data within it. This will lead to a higher consumer trust, and thanks to GDPR I believe a compliant company will have it easier to gain new clients but also to provide them with a better service.

Bron: https://eugdprcompliant.com/interview-state-secretary-privacy-belgium/

Of scan volgende QR code:

GDPR CHECKLIST – PART 3 – IT GOVERNANCE AND CONTROL PROCEDURES

April 4, 2018 in Compliance, GDPR and Business by Kevin Bollengier 0 Comments

THE IMPORTANCE OF A GOOD IT GOVERNANCE STRUCTURE

IT governance is a framework that helps you align your IT strategy with your business strategy and goals. There are tons of great examples out there like COBIT, ISO and more. GDPR will require a change in the habits of your employees. But as a company you need to establish clear guidelines and standards. It's also very important to audit these standards to maintain compliant to both internal and external factors.

INFORMATION SECURITY POLICIES

Part of good IT governance is having a good IT security management. It's of great value to have strong policies compliant to current standards. Unhashed passwords in a database, no password policy or not using SSL for sensitive forms for login or payments is not accepted in a digitalizing age. The first step to create good policies is to identify the risks that threaten your assets. This can be done by verifying the Confidentiality, Integrity and Availability (CIA) of an information asset.

Writing policies is one thing, but making them understandable for your employees is another. When creating policies, go in details but I also advice to make an IT manual. This IT manual contains bullet points of the "need to knows" and "how to's". For example a password policy will contain all the technical specifications but the IT handbook will just state the password requirements and how the password can be changed.

RISK INFORMATION MANAGEMENT

When creating policies, create control procedures. Having policies are only as strong as long they are complied with. These control procedures state how compliance towards a policy is measured, who is responsible for the audit and so on. The key element of a procedure is how often it is performed, so again based on a risk assessment, some policies require more frequent audits compared to others.

When an audit is performed, this should be logged along side any documentation and proof of compliance or non-compliance. Non-compliance should be escalated towards higher management to take counter measures.

THE LINK TO GDPR

One of the core tasks of GDPR is to analyze and deal with risks and threats. Performing risk & threat assessments, creating a strong IT strategy with corresponding policies, controls and audits will help you raise the overall level of information security in your business and minimalize the chances of encountering security and personal data breaches.

Bron: https://eugdprcompliant.com/gdpr-checklist-part-3-it-governance-and-control-procedures/

Of scan volgende QR code: