Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

GDPR

Het klokje tikt!
Wees voorbereid

Inger Verhelst &Stephanie Raets
Advocaten Claeys & Engels
PMClub 14 november 2017

Inleiding

De GDPR is in werking getreden op 25 mei 2016, maar zal pas van toepassing zijn vanaf 25 mei 2018

- Verordening 2016/679 betreffende de bescherming van natuurlijke personen i.v.m. de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG

  = **A**lgemene **V**erordening **G**egevensbescherming

  = **G**eneral **D**ata **P**rotection **R**egulation

- Nationale regels zullen een rol blijven spelen
  - Aanpassing nationale regelgeving verwacht

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

2

Inleiding

GDPR en HR

- In meeste niet-'data-driven' bedrijven: personeelsgegevens op grotere schaal verwerkt dan eender welke andere gegevens
- Vaak 'gevoelig' van aard
  - Bvb. lonen, evaluatieverslagen, enz.
- Niet optioneel, maar noodzakelijk voor het HR beleid, de payroll verwerking en het controlerecht van de werkgever dat er persoonsgegevens verwerkt worden
- Ondergeschikt verband heeft gevolgen
- GDPR-compliant zijn vergt kennis door en medewerking van het personeel

Claeys & Engels

3

Overzicht

- De basisprincipes en hun toepassing in de context van HR
- Praktische case

Claeys & Engels

De basisprincipes en hun toepassing in de context van HR

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

5

Basisprincipes

(bestaande principes grotendeels behouden)

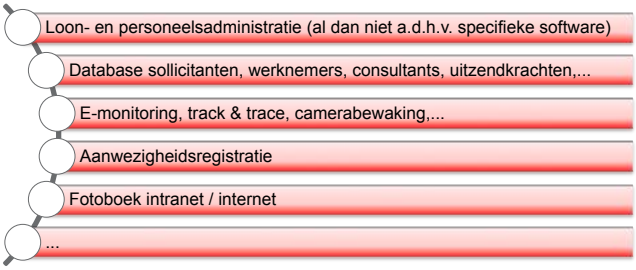
Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

6

1 Toepassingsgebied GDPR

Tal van verwerkingsactiviteiten in HR context

- Verwerking van alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (bv. sollicitanten, werknemers, uitzendkrachten, zelfstandigen ('freelancers', de consultants, de onderaannemers))
- (1) geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, en (2) de niet-geautomatiseerde verwerking die in een bestand zijn opgenomen of die zijn bestemd om daarin te worden opgenomen
- Voorbeelden



Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

7

2 Key players

"Verwerkingsverantwoordelijke" *("Data controller")*

- Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt
- Voorbeelden: de onderneming, de IBP, de moedervennootschap, de holding,...
- Joint controllers

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

8

Key players

"Verwerker" *("Data processor")*

- Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt
- Voorbeelden: het sociaal secretariaat m.b.t. payroll, dienstverleners (bv. archiveringsdiensten),...

Claeys & Engels

9

3 Overkoepelende principes

Principe	Huidige wetgeving	GDPR
Doelbinding	De gegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld	Rechtvaardigt de verwerking voor andere doeleinden dan de initiële indien de verwerking verenigbaar is met de doeleinden waarvoor de gegevens initieel zijn verzameld – evaluatie van de verenigbaarheid door de verwerkingsverantwoordelijke Verenigbaarheid niet vereist indien juridische basis voor de verwerking + toestemming of EU/nationaal recht
Juistheid	Gegevens moeten nauwkeurig zijn en indien nodig up-to-date gebracht worden Alle redelijke maatregelen moeten genomen worden om onjuiste gegevens te verwijderen/verbeteren	
Integriteit en vertrouwelijkheid	Verwerking moet passend beveiligd worden middels passende technische of organisatorische maatregelen	Dit wordt een basisprincipe

Claeys & Engels

10

Overkoepelende principes

Principe	Huidige wetgeving	GDPR
Rechtmatige, behoorlijke en transparante verwerking	Principes bestaan reeds Versterkt transparantiebeginsel: alle informatie of elke communicatie met betrekking tot de verwerking van de gegevens moet gemakkelijk toegankelijk en te begrijpen zijn	
Minimale gegevensverwerking	De gegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt	Het principe werd niet zo bestempeld, maar bestond reeds. Het doel van dit principe is dat de verwerkingsverantwoordelijke enkel die gegevens verwerkt die onmisbaar zijn voor het vooropgestelde doel. Men mag dus enkel het strikte minimum verwerken.
Opslagbeperking	De gegeven moeten in een vorm worden bewaard die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is	

Claeys & Engels

11

4 Relevante rechtsgronden

1. Toestemming
2. Noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor de uitvoering van de precontractuele maatregelen op verzoek van betrokkenen
3. Noodzakelijk o.w.v. wettelijke verplichting
4. Noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verantwoordelijke of een derde mits de belangen of de grondrechten en fundamentele vrijheden van de betrokkene niet zwaarder doorwegen
   - Voorbeeld (< preambule GDPR): doorzending van persoonsgegevens binnen concern voor interne administratieve doeleinden

Claeys & Engels

12

Relevante rechtsgronden

Toestemming als rechtsgrond

- Belang vrije toestemming
  - Wanverhouding tussen verwerkingsverantwoordelijke en betrokkene
  - Uitvoering overeenkomst afhankelijk van toestemming zonder dat die noodzakelijk is voor die uitvoering
- TO DO
  - Bereid de documenten met betrekking tot de noodzakelijke informatie voor de toestemming op voorhand voor
  - Indien mogelijk, andere rechtsgrond voorzien voor de verwerking en de toestemming beschouwen als een bijkomende rechtsgrond

Claeys & Engels

13

5 Bijzondere categorieën

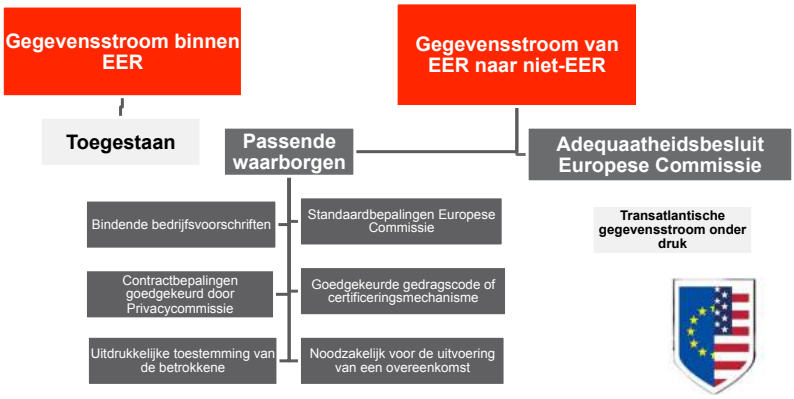
Gevoelige persoonsgegevens

- Voorbeelden
  - Waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken
  - Gegevens over gezondheid
  - Gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (bv. uittreksel strafregister)
- Principieel verbod van verwerking
- Specifieke uitzonderingen

Claeys & Engels

14

6 Doorgifte aan landen buiten Europa



Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

15

Belangrijke wijzigingen

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

16

1 Ruimere rechten voor betrokkenen

- Recht van inzage
- Recht op rectificatie
- Recht op gegevensuitwissing (‘*right to be forgotten*’)
- Recht op beperking van de verwerking van gegevens (‘*right to freeze*’)
- Recht op overdraagbaarheid van gegevens (‘*data portability*’)
- Recht van bezwaar
- Geautomatiseerde individuele besluitvorming

Claeys & Engels

17

Ruimere rechten voor betrokkenen

- To do 
  - Opleiding aan de verantwoordelijken omtrent de rechten
  - Informatie aan de betrokkenen: privacy notice / policy

Claeys & Engels

18

2 Meer verplichtingen voor verwerkingsverantwoordelijke

2.1 Uitgebreide informatieverplichting

- Bestaand:
  - Coördinaten van de verwerkingsverantwoordelijke
  - Doeleinden van de verwerking
  - (Categorieën van) ontvangers van de gegevens
  - Al dan niet verplicht karakter van antwoord en eventuele gevolgen (indien gegevens bij betrokkene opgevraagd)
  - (Categorieën van) gegevens (indien niet rechtstreeks van betrokkene verkregen
  - Recht op toegang en verbetering
  - Uitbreiding

2 Meer verplichtingen voor verwerkingsverantwoordelijke

Uitgebreide informatieverplichting

- Uitbreiding
  - Rechtsgrond om de gegevens te verwerken: *impliceert voorbereiding door de onderneming*
  - Indien van toepassing, informatie omtrent de intentie de gegevens te versturen naar een derde land of naar een internationale organisatie + info over passende bescherming
  - Opslagtermijn (of criteria ter bepaling ervan)
  - Recht op gegevensoverdraagbaarheid
  - Recht op inzage, rectificatie, wissing, beperking, bezwaar
  - Recht om toestemming in te trekken
  - Recht om klacht in te dienen bij Gegevensbeschermingsautoriteit
  - In voorkomend geval: coördinaten *Data Protection Officer*
  - In voorkomend geval: informatie over geautomatiseerde besluitvorming

Meer verplichtingen voor de verwerkingsverantwoordelijke

Uitgebreide informatieverplichting

- TO DO :

  - Voorbereiden van template documenten rekening houdend met de verschillende hypothesen:

    - Informatie aan de sollicitanten
    - Informatie aan de nieuw aangeworven werknemers
    - Informatie aan de werknemers die reeds in dienst zijn

Claeys & Engels

21

Meer verplichtingen voor de verwerkingsverantwoordelijke

2.2 Documentatieplicht – register van de verwerkingsactiviteiten

- Vervanging van de aangifteplicht bij de Gegevensbeschermingsautoriteit

  - Doel = vermindering van de administratieve lasten
  - Vaststelling: aangiften vinden zelden plaats en registers met vermeldingen worden zelden gepubliceerd
  - Belgische wet moet nog worden aangepast

- Van toepassing op het merendeel van de bedrijven

Claeys & Engels

22

Meer verplichtingen voor de verwerkingsverantwoordelijke

Register van de verwerkingsactiviteiten

- *De facto* van toepassing op het merendeel van de ondernemingen
  - De verplichting is van toepassing op de verwerkingsverantwoordelijke en de verwerker
  - Verplichtingen voor de ondernemingen met minstens 250 *werknemers* in dienst
  - Moeten de ondernemingen en bedrijven met minder dan 250 werknemers een register bijhouden? Enkel indien:
    - De verwerking mogelijk een risico inhoudt voor de rechten en vrijheden van de betrokkenen
    - Verwerking niet occasioneel is– wat zegt de Gegevensbeschermingsautoriteit daar *momenteel* over?
      - Toevallige, incidentele verwerking v. gebruikelijk
      - Zijn geen occasionele verwerkingen: verwerkingen gelinkt aan het beheren van het cliënteel / beheren van het personeel / beheren van de leveranciers
    - Verwerking van gevoelige informatie
    - Verwerking van juridische informatie
- Aanbeveling van de Gegevensbeschermingsautoriteit
  Zelfs indien niet verplicht, *best practice* (verantwoordingsplicht)

Claeys & Engels

23

Meer verplichtingen voor de verwerkingsverantwoordelijke

Register van de verwerkingsactiviteiten

- Hoe moet het register worden opgesteld?
  - Schriftelijk
  - Mag elektronisch zijn
  - Niet noodzakelijk om papieren versie + elektronisch te cumuleren
  - "Dynamische" verplichting: register moet op een continue manier up-to-date worden gehouden
  - Het moet duidelijk en verstaanbaar zijn voor de Gegevensbeschermingsautoriteit die het op elk moment mag opvragen
  - Niet-bindend model ter beschikking gesteld door de Gegevensbeschermingsautoriteit

Claeys & Engels

24

Meer verplichtingen voor de verwerkingsverantwoordelijke

Register van de verwerkingsactiviteiten

- Informatie die moet worden opgenomen in het register:

1. naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming
2. verwerkingsdoeleinden
3. beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens
4. categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties
5. indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, indien toepasselijk, de documenten inzake de passende waarborgen
6. indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist
7. indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen

Meer verplichtingen voor de verwerkingsverantwoordelijken

Register van de verwerkingsactiviteiten

- TO DO : 
  - Opstellen van dit register van de verwerkingsactiviteiten
- Moeilijk te vermijden nu de Gegevensbeschermingsautoriteit van oordeel is dat de verwerkingen die betrekking hebben op het personeelsbeheer geen occasionele verwerkingen zijn

Meer verplichtingen voor de verwerkingsverantwoordelijken

2.3 Verplichting tot aanduiding van een functionaris voor gegevensbescherming ("*Data Protection Officer*")

		Verplicht	Facultatief
1	Overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken	✔	
2	Gerechten bij de uitoefening van hun rechterlijke taken		✔
3	Core activity = grootschalige verwerking van gevoelige gegevens en gegeven m.b.t strafrechtelijke veroordelingen en strafbare feiten	✔	
4	Core activity = verwerkingen die vanwege hun aard, omvang en/of doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen	✔	
5	Privésector: niet in de hypotheses 3 en 4		✔

Claeys & Engels

27

Meer verplichtingen voor de verwerkingsverantwoordelijken

2.4 Striktere beveiligingsmaatregelen voor persoonsgegevens

- **Gegevensbeschermingseffectbeoordeling** ('**DPIA**')
  - Indien min. 2 van de volgende 9 criteria van toepassing zijn

Evalueren/toekennen van een score (profiling/ voorspellen)	*Matchen of combineren van datasets*
Automatische besluitvorming met gevolgen	*Kwetsbare betrokkenen*
Systematische monitoring	*Innovatieve oplossingen*
Gevoelige gegevens	*Verwerking kan leiden tot uitsluiting van rechten*
Grootschalige verwerking	

Claeys & Engels

28

Meer verplichtingen voor de verwerkingsverantwoordelijken

Striktere beveiligingsmaatregelen voor persoonsgegevens

- De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke (en toegang heeft tot persoonsgegevens) deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij Unierechtelijk of lidstaatrechtelijk tot de verwerking is gehouden
- TO DO : 
  - Vorming van het personeel
  - Opstellen van een beleid om aan te tonen dat in geval van controle/probleem het personeel werd gesensibiliseerd

Meer verplichtingen voor de verwerkingsverantwoordelijken

2.5 Verplichting om de inbreuken te documenteren en te melden

- Risico voor de rechten en vrijheden van de betrokken personen ≠ risico voor de onderneming
- Melding
  - aan de toezichthoudende autoriteit – zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur na kennisname;
  - en, in bepaalde gevallen, aan de betrokkenen – zonder onnodige vertraging

Meer verplichtingen voor de verwerkingsverantwoordelijken

Verplichting om de inbreuken te documenteren en te melden

- TO DO : 
  - Intern beleid en vorming
  - Op voorhand modeldocumenten voor de melding van een inbreuk i.v.m. persoonsgegevens opstellen
  - Houd rekening met zeer korte termijnen

Claeys & Engels

31

Meer verplichtingen voor de verwerkingsverantwoordelijken

2.6 Due diligence van verwerkers en schriftelijke overeenkomst

- Keuze van verwerker – nodige garanties
- Verwerker mag niet handelen als een verwerkingsverantwoordelijke
  - Risico: aansprakelijkheid als verwerkingsverantwoordelijke

Claeys & Engels

32

Meer verplichtingen voor de verwerkingsverantwoordelijken

Due diligence van verwerkers en schriftelijke overeenkomst

- Schriftelijke overeenkomst noodzakelijk

  - Onderwerp + duur verwerking
  - Aard + doel verwerking
  - Soort persoonsgegevens
  - Categorieën van betrokkenen
  - Rechten en verplichtingen van de verwerkingsverantwoordelijke
  - Verplichtingen van de verwerker
    - Instructies respecteren
    - Ervoor zorgen dat de mensen die bevoegd zijn om persoonsgegevens te verwerken, zich ertoe verbinden om de vertrouwelijkheid te respecteren of aan een gepaste wettelijke verplichting tot vertrouwelijkheid zijn onderworpen
    - Gepaste beveiligingsmaatregelen nemen

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

33

Meer verplichtingen voor de verwerkingsverantwoordelijken

Due diligence van verwerkers en schriftelijke overeenkomst

- Schriftelijke overeenkomst noodzakelijk
  - Verplichtingen van de verwerker *(vervolg)*
    - aan de voorwaarden voor het in dienst nemen van een andere verwerker voldoen
    - de verwerkingsverantwoordelijke bijstand verlenen bij het doen nakomen van zijn verplichtingen (o.m. m.b.t. rechten betrokkenen)
    - na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wissen, terugbezorgen en kopieën verwijderen
    - de verwerkingsverantwoordelijke alle informatie ter beschikking stellen die nodig is om de nakoming van zijn verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een andere controleur mogelijk maken en eraan bij te dragen,

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

34

3 Eén-loketmechanisme – “One Stop Shop”

- Ondernemingen die zaken doen in verschillende lidstaten van de EU moeten voortaan werken met één centraal loket
- Leidende toezichthoudende autoriteit
  - Hoofdvestiging
  - Tenzij data protection beslissingen worden genomen in een
- Zogenaamd ‘grote vernieuwing’
- Moet toch gerelativeerd worden, zeker in HR

Claeys & Engels

35

4 GDPR – Groter risico op sancties

4.1 Onderzoeksbevoegheid

- Inspectiedienst binnen Gegevensbeschermingsautoriteit
- Bevoegdheden
  - verwerkingsverantwoordelijke en verwerker gelasten alle voor de uitvoering van haar taken vereiste informatie te verstrekken
  - onderzoeken verrichten in de vorm van gegevensbeschermingscontroles (“audits”)
  - toegang krijgen tot alle bedrijfsruimten van de verwerkingsverantwoordelijke en zijn verwerker

Claeys & Engels

36

GDPR – Groter risico op sancties

4.2 Sanctiebevoegheid van de Gegevensbeschermingsautoriteit

- Gegevensbeschermingsautoriteit kan sancties opleggen!
- Afschrikwekkende boetes - schematisch

Inbreuk op de verplichtingen van de verwerkingsverantwoordelijke	**Inbreuk op:** - **algemene principes van gegevensbescherming** - **de rechten van de betrokken personen**
Maximum 10 000 000 EUR OF 2% van de wereldwijde jaaromzet van het voorgaande boekjaar	Maximum 20 000 000 EUR OF 4% van de wereldwijde jaaromzet van het voorgaande boekjaar

- Mogelijkheid om rekening te houden met verzachtende of verzwarende omstandigheden

Claeys & Engels

37

GDPR – Groter risico op sancties

Sanctiebevoegheid van de Gegevensbeschermingsautoriteit

- Andere mogelijke corrigerende maatregelen
  - Waarschuwing
  - Berisping
  - Verplichting om verzoeken tot uitoefening van rechten in te willigen
  - Verplichting om verwerkingen in overeenstemming te brengen met de bepalingen van de GDPR
  - Verplichting om een inbreuk in verband met de persoonsgegevens aan de betrokken persoon mee te delen
  - Tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod
  - Verplichting tot rectificatie of de wissing van persoonsgegevens
  - Verplichting tot opschorting van gegevensstromen naar een derde land
- Gekwalificeerd door de Gegevensbeschermingsautoriteit zelf als maatregelen die mogelijks "*een groter afschrikkend effect hebben dan het opleggen van een administratieve geldboete*"

Claeys & Engels

38

GDPR- Groter risico op sancties

4.3 Andere maatregelen

- Mogelijkheid voor de betrokken persoon om een klacht in te dienen bij de Gegevensbeschermingsautoriteit indien deze van oordeel is dat de verwerking van zijn persoonsgegevens de GDPR schendt
- Mogelijkheid om een schadevergoeding te vorderen voor de gerechten
- Algemeen principe: omkering bewijslast (verantwoordingsplicht verwerkingsverantwoordelijke)

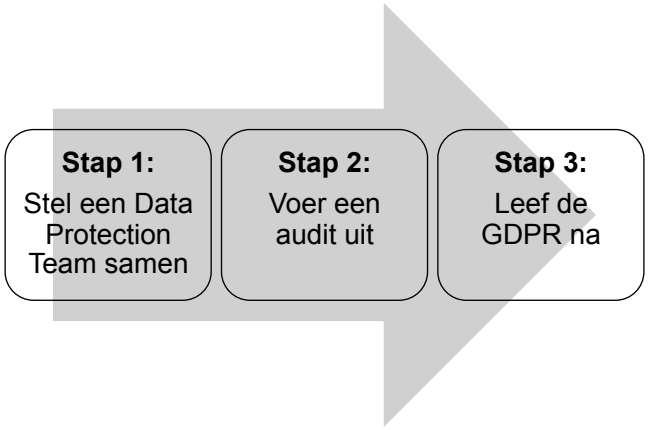
Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

39

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

40

TO DO



Claeys & Engels

41

TO DO

- Stap 1: Stel een Data Protection Team samen
  - Duid in uw onderneming personen aan die deel zullen uitmaken van dit team en zullen instaan voor de voorbereiding
  - Zorg ervoor dat het team multidisciplinair is (HR, IT, juristen, anderen?)
  - Voorzie hen van voldoende middelen en opleiding
- Stap 2: Voer een audit uit
  - Lijst de verschillende data flows op
  - Nagaan welke gegevens er worden verwerkt, voor welke doeleinden, met welke bewaringstermijn en indien de onderneming optreedt als zijn eigen verwerkingsverantwoordelijke of als zijn verwerker...
  - Elk van deze vragen heeft immers zijn eigen gevolgen voor hetgeen noodzakelijk is voor de naleving van de GDPR (stap 3).

Claeys & Engels

42

TO DO

- Stap 3: Naleving van de GDPR

Op basis van de mapping :

- Wettelijke basis voor elke verwerking nagaan en een register van alle verwerkingsactiviteiten opmaken
- Beveiligingsmaatregelen ontwikkelen
- 'Privacy notices' en overeenkomsten met verwerkers aanpassen/opstellen
- Wettelijke basis voor de internationale gegevensstromen nagaan en eventueel passende contractuele waarborgen aanpassen/opstellen
- Functionaris voor gegevensbescherming aanstellen (indien nodig of gewenst)
- Specifieke policies aanpassen/opstellen (bvb.: ICT-policy, geo-policy, camerapolicy...).

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

43

Praktische case

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

44

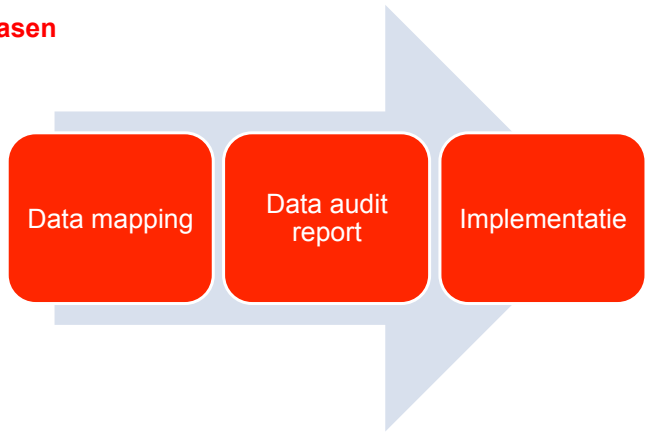
Case: Audit verwerkingsactiviteiten

Data protection audit

- **Buzzibuzzi nv** maakt deel uit van de wereldwijde Buzzi-groep, waarvan de moederonderneming **Buzzibuzzi Inc. in Amerika** gevestigd is. De moederonderneming heeft in 2010 beslist dat alle vestigingen wereldwijd gebruik moeten beginnen maken van **PerfApp**, een software waarin de evaluaties van het personeel moeten worden bewaard. Een kenmerk van de software is dat de daarin opgeslagen gegevens van overal kunnen worden geraadpleegd, ook vanuit Amerika. Buzzibuzzi nv past het systeem sinds 2011 toe zonder ooit de 'data protection' aspecten ervan in vraag te hebben gesteld. Nu plant ze dat toch te doen in het kader van de GDPR compliance oefening.

Case: Audit verwerkingsactiviteiten

Drie fasen



Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **a) Beschrijving verwerkingsactiviteit (‘*Business process*’):**

Gebruik van software PerfApp voor de evaluatie van het personeel

Claeys & Engels

47

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**

  - (1) Doel
  - (2) Betrokkenen (categorieën)
  - (3) Persoonsgegevens
  - (4) Verzamelen van de gegevens
  - (5) Grond voor gegevensverwerking (wettigheid)
  - (6) Bewaring
  - (7) Locatie van bewaring

Claeys & Engels

48

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - (8) Toegangsrechten
  - (9) Gegevensoverdracht buiten de EU (in de groep)
  - (10) Bewaartermijn
  - (11) Aangifte bij Privacycommissie/Gegevensbeschermingsautoriteit
  - (12) Worden de betrokkenen geïnformeerd over de gegevensverwerking, en hoe?
  - (13) Technische en organisatorische beveiligingsmaatregelen
  - (14) Incidenten/geschillen in het verleden

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(1) Doel***
    - Beheer van het personeel en de tussenpersonen
  - ***(2) Betrokkenen (categorieën)***
    - Huidig personeel
    - Voormalig personeel

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(3) Persoonsgegevens***
    - Identificatiegegevens.
      - Persoonlijke identificatiegegevens: naam, titel, adres (privé, werk), vroegere adressen, telefoonnummer (privé, werk), identificatiegegevens toegekend door verantwoordelijke.
    - Persoonlijke kenmerken
    - Persoonlijke bijzonderheden: leeftijd, geslacht, geboortedatum, nationaliteit.
    - Gegevens i.v.m. 'Beroep en betrekking':
      - Huidige betrekking, aanwerving, loopbaan, aanwezigheid en discipline, organisatie van het werk, evaluatie, vorming tot de functie, evaluatie van het gebruik van de informaticamiddelen (internet, e-mail,....)

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(4) Verzamelen van de gegevens***
    - Via de werknemer
    - Gegenereerd door de leidinggevenden en HR
  - ***(5) Grond voor gegevensverwerking (wettigheid)***
    - Noodzakelijk voor de uitvoering van de arbeidsovereenkomst met de betrokken werknemers (gezagsrecht werkgever)
    - Noodzakelijk in het kader van het gerechtvaardigd belang van de werkgever, meer bepaald in het kader van het toezicht op de uitvoering van de arbeidsovereenkomst door de werknemer.

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(6) Bewaring***
    - De gegevens worden in elektronische vorm bewaard
  - ***(7) Locatie van bewaring***
    - Via een web applicatie / software
    - De server bevindt zich in Amerika

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(8) Toegangsrechten***
    - De persoonsgegevens van de werknemers opgeslagen in PerfApp zijn toegankelijk voor:
      - De leidinggevenden die enkel aan de gegevens van de werknemers van hun eigen team kunnen over wie zij een beoordelingsbevoegdheid hebben
      - De medewerkers van het HR departement die tot alle gegevens toegang hebben
      - De medewerkers van het IT departement die ook tot alle gegevens toegang hebben

    Deze personen kunnen, ingevolge de Matrix-structuur ook in Amerika gevestigd zijn.

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(9) Gegevensoverdracht buiten de EU (in de groep)***
    - Ja, vanuit Amerika kunnen personeelsleden van Buzzibuzzi Inc. zich toegang verschaffen tot de gegevens.
    - Daarvoor zijn geen bijzondere waarborgen genomen.

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(10) Bewaartermijn***
    - De persoonsgegevens in PerfApp worden (voorlopig) onbeperkt bewaard, ook m.b.t. werknemers die niet langer in dienst zijn.
  - ***(11) Aangifte bij Privacycommissie/Gegevensbeschermingsautoriteit***
    - Buzzibuzzi nv heeft geen aangifte bij de Gegevensbeschermingsautoriteit gedaan m.b.t. PerfApp.

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(12) Worden de betrokkenen geïnformeerd over de gegevensverwerking, en hoe?***
    - Er staat een zin in de arbeidsovereenkomst: "*De werknemer erkent dat de werkgever van hem/haar persoonsgegevens zal verwerken in het kader van de arbeidsovereenkomst*".
  - ***(13) Technische en organisatorische beveiligingsmaatregelen***
    - Technische maatregelen
    - Paswoord beveiliging
    - Lijst van gemachtigde personeelsleden
    - Toezicht, controle en onderhoud

Claeys & Engels

57

Case: Audit verwerkingsactiviteiten

STAP 1 – Data mapping *(high level)*

- **b) Details verwerkingsactiviteit**
  - ***(14) Incidenten/geschillen in het verleden***
    - Er zijn in het verleden nog geen incidenten of geschillen geweest die betrekking hebben op deze verwerkingsactiviteit.

Claeys & Engels

58

Case: Audit verwerkingsactiviteiten

STAP 2 – Data audit report *(high level)*

Claeys & Engels

59

Case: Audit verwerkingsactiviteiten

STAP 3 – Implementatie

- **Passende waarborgen data transfer Amerika**
  - Bijvoorbeeld: standaard contractuele bepalingen
- **Aangepaste toegangsrechten**
  - Bijvoorbeeld: voortaan enkel lead HR en lead IT, ondergeschikt personeel enkel in specifieke gevallen en mits een specifieke autorisatie

Claeys & Engels

60

Case: Audit verwerkingsactiviteiten

STAP 3 – Implementatie

- **Retentiebeleid**
  - Bijvoorbeeld: gegevens voormalig personeel voortaan verwijderd één jaar na beëindiging arbeidsrelatie (behalve in geval van geschillen)
- **Passende informatie**
  - Bijvoorbeeld: opstellen van een algemene Privacy Notice aan de werknemers waar deze verwerkingsactiviteit door gedekt wordt

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

61

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

62

Bezoek onze website

http://gdprbelgium.be/nl

De General Data Protection Regulation wordt van toepassing

Nog 247 dagen

Wat verandert er voor uw HR-beleid?

Claeys & Engels

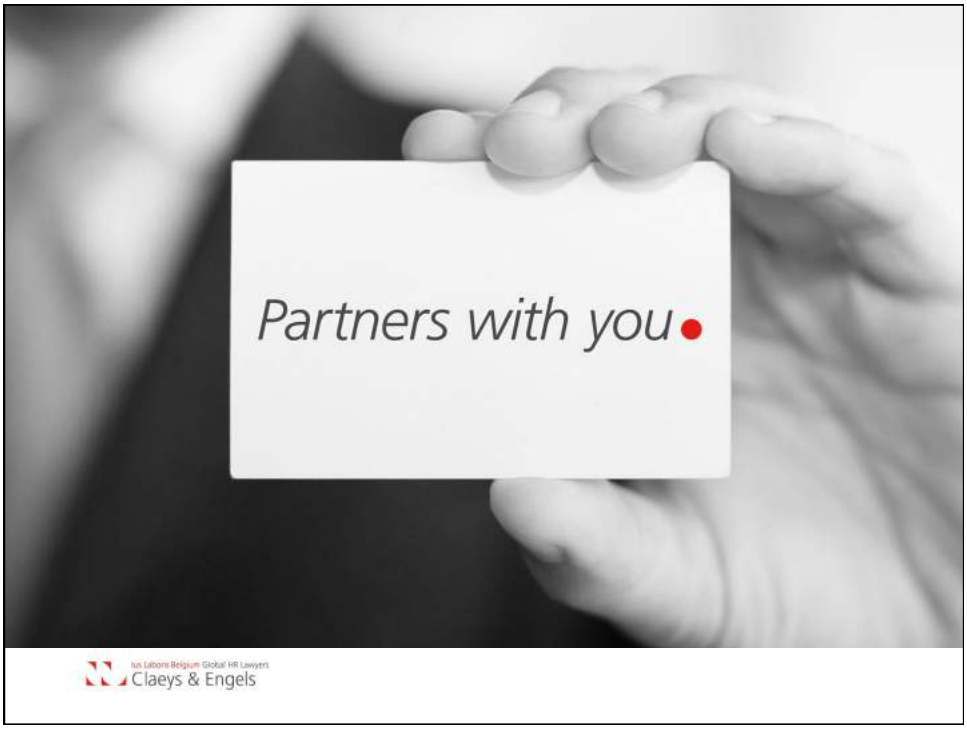
63

Contact

Inger Verhelst
Avocaat - Vennoot
Claeys & Engels
inger.verhelst@claeysengels.be
T +32 3 285 97 82

Stephanie Raets
Avocaat - Senior Associate
Claeys & Engels
stephanie.raets@claeysengels.be
T +32 3 285 97 90

Claeys & Engels



Ius Laboris Belgium Global HR Lawyers
Claeys & Engels