Academiejaar 2018-2019

Scriptie voorgedragen door:
Nassima El Kindi
0683114

Privacy awareness

Wat moeten werknemers weten wat betreft privacy?

Tot het behalen van het diploma van Bachelor in het Bedrijfsmanagement
Afstudeerrichting: **Rechtspraktijk**

Promotor: Tim Greven

Inhoudsopgave

Woord vooraf

Het schrijven van deze scriptie was een leerrijke ervaring die mij heeft toegestaan een verder begrip te krijgen over de General Data Protection Regulation binnen de bedrijfswereld. Zonder de hulp van vele mensen, zou ik deze scriptie nooit tot een goed einde kunnen brengen. Bij deze, wil ik graag iedereen bedanken.

Mijn moeder Sofia El Ouariachi voor haar oneindige steun en geduld. Zonder de kansen die ze mij gaf, zou ik vandaag niet staan waar ik nu sta.

Mijn promotor Meneer Tim Greven voor de fantastische begeleiding en ondersteuning, maar ook voor de levenslessen van de voorbije drie jaar. U heeft het verschil gemaakt.

Mijn stagementor Liselotte Leenaerts voor al de informatie en de aanwijzingen die mij in staat hebben gesteld mijn scriptie af te werken.

Mijn Ordina collega's en al mijn vrienden voor de morele steun en de goede raad.

Abstract

We leven in een digitaliserende en snel evoluerende wereld op het gebied van informatietechnologie. Bij digitalisering zijn natuurlijk veel gegevens aanwezig, inclusief persoonsgegevens. De opkomst van de General Data Protection Regulation (GDPR) bracht sterkere privacyrechten met zich mee en streefde ernaar de persoonsgegevens van de Europese burgers beter te beschermen. Bovendien zijn alle bedrijven die persoonsgegevens van Europese burgers verwerken, onderworpen aan deze nieuwe wetgeving. Eén van de vele stappen die bedrijven moeten nemen om GDPR compliant te worden, is het creëren van privacy awareness op de werkvloer. Dit wordt door veel bedrijven erkent als de moeilijkste stap om te nemen. Ik nam het dus verder onder de loep en ging op onderzoek uit.

Verklarende woordenlijst

GDPR: General Data Protection Regulation of GDPR is de wet 2016/679. De wet stipuleert de nieuwe regels voor databescherming. De wet telt 99 artikelen.

Persoonsgegevens: Persoonlijke informatie van een persoon waarbij hij of zij geïdentificeerd kan worden.

Verwerken: is elke handeling met betrekking tot persoonsgegevens waarbij deze worden verzameld, geordend, bewaard, gewijzigd, opgevraagd, geraadpleegd, gebruikt, verspreid, gewist en vernietigd.

Verwerkersverantwoordelijke: is een organisatie of een persoons die de doeleinden en de middelen van de verwerking van persoonsgegevens bepaalt.

Verwerker: is een externe partij die verwerkingen uitvoert in opdracht van de verwerkingsverantwoordelijke.

Betrokkene: is de identificeerbare natuurlijk persoon op wie de verwerkte persoonsgegevens betrekking hebben.

DPIA: Data Protection Impact Assessment of gegevensbeschermingseffectbeoordeling is een procedure om te evalueren of een verwerking van persoonsgegevens een risico inhoudt voor de rechten en vrijheden van de betrokkene.

Verwerkingsregister: Iedere verwerkingsverantwoordelijke of verwerker moet een verwerkingsregister bijhouden, die volgende gegevens moet bevatten: contactgegevens van de verwerkingsverantwoordelijke, verwerkingsdoeleinden, categorieën van de verwerkte persoonsgegevens, categorieën van betrokkenen en ontvangers.

Compliant: In regel zijnde met.

DPO: Data Protection Officer is de nieuwe positie die in het leven is geroepen door de General Data Protection Regulation (GDPR). De DPO zal zich voornamelijk bezighouden met het toezien op de correcte naleving van de GDPR.

GBA: De Gegevensbeschermingsautoriteit of GBA is een onafhankelijk orgaan dat erop toeziet dat de basisbeginselen van de bescherming van de persoonsgegevens correct worden nageleefd.

Working Group 29: is een onafhankelijke Europese werkgroep die de intreding van de GDPR verantwoordelijk was voor de behandeling van kwesties in verband met gegevensbescherming.

Pseudonimiseren: Met pseudonimiseren worden persoonsgegevens vervangen door versleutelde gegevens.

Encryptie: is voor het coderen van gegevens.

Hacker: Wordt ook wel een cracker genoemd, is een persoon die binnendringt in computernetwerken door de beveiligingssystemen te omzeilen.

Inleiding

"The individual shall have full protection in person and in property." -Brandeis and Warren

Wat betekent onze privacy vandaag eigenlijk nog in een wereld met sociale media, digitalisering en het steeds groter wordende - mis(ge)bruik van data?

Om hier een volwaardig antwoord op te bieden kwam de Europese Unie met een verordening om de persoonsgegevens van ons allen te beschermen. De inwerkingtreding van de 'General Data Protection Regulation' (GDPR) bracht heel wat veranderingen met zich mee. Die veranderingen hielden een aantal verplichte regels in voor diverse actoren, om die reden werd GDPR een 'hot topic'. Voor het naleven en toepassen van deze regels, is 'privacy awareness' van groot belang. 'Awareness' of bewustwording creëren binnen een organisatie is namelijk één van de eerste stappen die men moet nemen om als organisatie grip te houden op de nieuwe wetgeving.

De GDPR is van toepassing op alle natuurlijke personen - zowel op klanten als op werknemers - en dat laatste wordt vaak vergeten. De GDPR heeft een belangrijke impact op de manier waarop werkgevers de persoonsgegevens van hun werknemers verwerken. Werkgevers beseffen vaak niet hoeveel verwerkingsprocedés er van toepassing zijn binnen hun bedrijf. Alleen de HR-werknemers bijvoorbeeld hebben al toegang tot heel wat persoonsgegevens zoals de loon- en personeelsadministratie en persoonlijke gegevens van alle sollicitanten.

Sinds de intreding van de GDPR zijn veel bedrijven serieus aan de slag gegaan met 'awareness' of bewustzijnscampagnes en trainingen van hun werknemers. Maar hebben al die bewustwordingsinitiatieven effect? In welke mate zijn werknemers privacy bewust? Wat houdt een bewustwordingsinitiatief juist in? En hoe zit het met de GDPR binnen de arbeidscontext? Worden de werknemers wel juist geïnformeerd over hun voorziene rechten? En weten ze hoe ze deze rechten ook in de praktijk kunnen toepassen?

Op al deze verschillende vragen zal hierna getracht worden een antwoord te formuleren. Dat antwoord zal echter onvermijdelijk soms gepaard gaan met technisch jargon, dat in de mate van het mogelijke beperkt zal worden tot een minimum. De antwoorden op de onderzoeksvragen zullen in eerste instantie gezocht worden binnen het theoretische kader, daarnaast ga ik uitgebreid in op het praktijkonderzoek dat ik binnen het stagebedrijf kon voeren.

1. GDPR

1.1 Situering

1.1.1 EVRM

Het recht op bescherming van persoonsgegevens maakt deel uit van de eerbiediging op privéleven. Het recht op privéleven is een klassiek vrijheidsrecht dat de bescherming van privacy beoogt. Mensen hebben recht op een rechtmatige verwerking van hun persoonsgegevens om geen nadeel te ondervinden.

Een onrechtmatige verwerking van persoonsgegevens zou grote gevolgen met zich mee kunnen brengen voor individuen. Bijgevolg is het recht op privéleven een fundamenteel recht dat terug te vinden is in artikel 8 van het EVRM.[1]

1.1.2 OESO-Richtlijn

Van groot invloed was de opkomst van de Organisation for Economic Co-operation and development richtlijnen, ook wel bekend als OESO richtlijnen. De OESO, in samenwerking met de Raad van Europa, bracht de OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data uit.

Deze richtlijnen leggen regels vast over de bescherming van persoonlijke gegevens en privacy, met als doel de eenheid te bevorderen op dit gebied. De principes die daaruit vloeiden zijn van grote invloed geweest en zijn nog steeds in de GDPR terug te vinden.[2]

1.1.3 Belgische Privacywetgeving

Op nationaal niveau speelde de Wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens een belangrijke rol. Het had als doel de burgers te beschermen tegen mogelijke misbruik van hun persoonsgegevens. De wet voorzag zowel de rechten en plichten van de betrokken persoon, als de rechten en plichten voor de verwerker. Eveneens werd de Privacycommissie aangesteld.

Op grond van deze wet werd de Privacycommissie een onafhankelijke instantie die toeziet op het zorgvuldig en beveiligd gebruik van de persoonsgegevens, met als doel het blijven waarborgen van de privacy van de burgers. Bovendien kon de Privacycommissie optreden als bemiddelaar bij klachten tussen de verwerkers en de betrokkenen, alsook bijstand en toelichting verlenen.[3]

Deze wetgeving was niet langer up to date met onze hedendaagse vorm en snelheid van het verwerken van persoonsgegevens.[4]

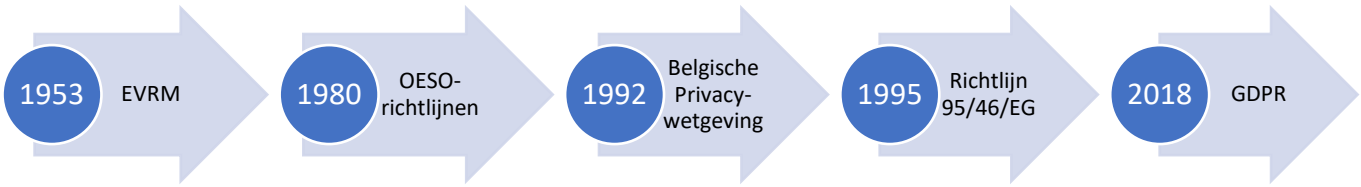
1.1.4 Richtlijn 95/46/EG van het Europees Parlement en De Raad

De databeschermingsrichtlijn of voluit *Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens* was een Europese Richtlijn die het verwerken van persoonsgegevens in de Europese Unie regelt. Het was een belangrijk deel van de EU-wetgeving over privacy.[5]

---

[1] Art. 8 EVRM.
[2] X, "Achtergrond van de AVG", https://avg-compleet.nl/blog/achtergrond-van-de-avg/, (consultatie 29 mei 2019).
[3] A. KEEREMAN, "Privacy moet voor bedrijven een uitgangspunt zijn", *DJK* 2015, nr. 307, 8-9.
[4] Gegevensbeschermingsautoriteit, "*Privacycommissie",* https://www.gegevensbeschermingsautoriteit.be/lexicon/privacycommissie, (consultatie 13 maart 2019); G. GOOSSENS en T. VAN CANNEYT, "The general data protection regulation: 10 things company lawyers should know", *CDJ* 2016, nr. 1, 1-11.
[5] 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Echter is deze richtlijn verouderd en paste niet meer bij het huidige digitale tijdperk. In 1995 had slechts 10% van de EU bevolking namelijk toegang tot internet. Er werd toen geen gebruik gemaakt van cookies, sociale media, mailings enzovoort. Hierdoor werd de databeschermingsrichtlijn op 25 mei 2018 vervangen door de GDPR.[6]



[6] R. SCHOEFS, "Witte rook voor nieuwe privacyverordening", *DJK* 2016, nr. 321, 16.

2.1 Wat is General Data Protection Regulation?

Het beheer en de beveiliging van persoonlijke gegevens van Europese burgers bestond reeds sinds de intreding van het EVRM en werd verder ontwikkeld tot in 1995 in de databeschermingsrichtlijn. De manier waarop men omging met persoonlijke data en hoe deze werden beveiligd was niet nader aangeduid. Dit leidde tot het creëren van een krachtig en coherenter wettelijk kader dat tegemoet komt aan de uitdagingen van de snelle technologische ontwikkelingen.

General Data Protection Regulation of ook Algemene Verordening Gegevensbescherming genoemd, is een geheel van regels die bescherming bieden op de persoonlijke gegevens van Europese burgers. De GDPR werd goedgekeurd op 14 april 2016 en trad effectief in werking op 25 mei 2018.[7]

Alvorens het bestaan van de GDPR hadden de Europese lidstaten elk hun eigen wetgeving omtrent privacy en veiligheid en het beschermen van persoonsgegevens van Europese burgers, wat aanleiding gaf tot onduidelijkheden en versnippering. De privacy werd toen geregeld op basis van de richtlijn 95/46/EG die omgezet moest worden in de nationale wetgeving. Hierdoor was er weinig sprake van harmonie en was er nood aan een uniform Europees kader op vlak van databescherming.

Doordat er nauwelijks duidelijke richtlijnen bestonden, hadden organisaties de vrijheid om data te verzamelen zonder duidelijke informatie te verstrekken aan de betrokken persoon. Daarnaast werd er geen toestemming gevraagd en werden de gebruikers verplicht om hun gegevens vrij te geven, indien ze gebruik wilden maken van de diensten.[8]

Deze problematiek leidde tot het opteren voor een verordening. Een verordening wordt gedefinieerd als *"een verordening heeft een algemene strekking. Zij is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat."*[9] Een verordening is hierdoor rechtstreeks van toepassing op alle lidstaten zonder dat het omgezet moet worden in nationale wetgeving. Dit zorgt voor de verkleining van de verschillen op de interne markt van Europa.

De territorialiteit van de GDPR werd ook uitgebreid naar het verwerken van persoonsgegevens door verwerkingsverantwoordelijken met een vestiging binnen de Europese Unie, zonder dat die verwerking in de Europese Unie zelf wordt uitgevoerd. De GDPR zal ook van toepassing zijn op de verwerkingsverantwoordelijke die gevestigd is buiten Europa, indien deze persoonsgegevens verwerkt voor het aanbieden van goederen of diensten aan derden binnen de Europese Unie.[10]

Aangezien de GDPR een aantal zaken bewust niet regelt, is het aan de lidstaten zelf om dit in te vullen. Een tussenkomst van Belgische wetgever was dan ook nodig. Op 5 september 2018 verscheen dit ook in de vorm van de 'kaderwet'.[11] Deze regelt een hele reeks privacymateries, waarbij ook de zogenaamde open clausules in de GDPR. Een voorbeeld hiervan is de leeftijd waarbij minderjarigen kunnen toestemmen met het verwerken van hun persoonsgegevens.[12] Tevens, zijn er bepaalde domeinen waarbij nationaal recht noodzakelijk is om uitzonderingen toe te laten op de rechten voorzien in de

---

[7] Y.S. VAN DER SYPE, "Bescherming van persoonsgegevens in de arbeidscontext anno 2018: enkele uitdagingen voor het rechtmatig verwerken van werknemersgegevens", *Arbeid. J.* 2017, 23-29; GDPR-eur, General Data Protection Regulation, https://gdpr-eu.be/wat-is-gdpr/, (consultatie 8 maart 2019); Europese Commissie, Gegevensbescherming in de EU, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_nl, (consultatie 8 maart 2019); Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 33/2018 van 11 april 2018; E. CRUYSMANS, "Data Protection & Privacy. Le GDPR dans la pratique", *RDIDC* 2018, nr. 2, 307-310.

[8] S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr. 7, 208.

[9] Art. 288 VWEU.

[10] M. DE BACKER en T. FRANSEN, "Algemene Verordening Gegevensbescherming. Naar een nieuw concept inzake bescherming van persoonsgegevens?", *NJW* 2018, nr. 378, 190-203.

[11] Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018.

[12] Art. 7 wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018.

GDPR. Een voorbeeld hiervan is het wetenschappelijk onderzoek op persoonsgegevens.[13] Tenslotte biedt de wet ook afwijkende regelingen voor overheidsinstanties en voor verwerkingen buiten het toepassingsgebied van de Europese Unie.[14]

2.2 Doelen

Het hoofddoel van de GDPR is het beschermen van persoonsgegevens van de Europese burgers. Dit gebeurt door meer controle te bieden aan de mensen over het verwerken van hun persoonsgegevens.

Bovendien is uniformiteit binnen de EU erg belangrijk. Om een consistent en hoog beschermingsniveau te kunnen handhaven, dient het niveau binnen de Europese Unie gelijkwaardig en coherent te zijn. Het vergemakkelijkt de naleving van de wet voor bedrijven die in meerdere EU-landen actief zijn. Daarnaast kan de rechtspraak beter op elkaar worden afgestemd. [15]

2.3 De toevoegingen

In tegenstelling tot wat de meeste denken, is de GDPR zoals we die vandaag kennen geen volkomen nieuwe regeling. De GDPR vervangt grotendeels de Belgische Privacywetgeving.[16] Toch brengen de nieuwe wijzigingen aanzienlijk wat gevolgen teweeg.[17]

2.3.1 Transparantie

De verwerkingsverantwoordelijke moet ervoor zorgen dat persoonsgegevens transparant worden verwerkt. Het transparantiebeginsel veronderstelt doorzichtigheid, duidelijkheid en zekerheid. Met andere woorden moet het volkomen duidelijk zijn voor de betrokken personen dat hun gegevens zijn ingezameld en zullen gebruikt of verwerkt worden. Dit beginsel vereist dat alle nodige informatie met betrekking tot gegevensverwerking gemakkelijk verstaanbaar en toegankelijk moet zijn. Daarnaast moeten de betrokkenen op de hoogte worden gebracht van zowel de mogelijke risico's en de regels, als de manier waarop ze hun rechten kunnen uitoefenen.[18]

2.3.2 Retentieperiode

Een probleem in de Belgische privacywetgeving was dat er geen bepaalde bewaartermijn was voor het verzamelen van data. De GDPR creëerde hiervoor een oplossing, namelijk dat persoonsgegevens van betrokkene niet langer worden bewaard dan noodzakelijk is voor het verwezenlijken van het doel waarvoor zij verwerkt worden. Deze retentieperiode dient op voorhand te worden vastgesteld. Dit had als gevolg dat bedrijven verplicht werden om duidelijk te stellen, dat er een retentieperiode is op de gegevens die ze verwerken.[19]

Echter, gelden hier ook bepaalde uitzonderingen. Conform artikel 89, kunnen gegevens voor langere tijd worden bewaard, indien de verwerking noodzakelijk is voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek. Hierbij heeft de wetgever passende waarborgen voorzien om te blijven voldoen aan het beginsel van "minimale

---

[13] Art. 99 wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018.
[14] T. BALTHAZAR, "Nieuwe kaderwet vormt sluitstuk voor GDPR", *De Juristenkrant* 2018, 1-2.
[15] Y.S. VAN DER SYPE, "Bescherming van persoonsgegevens in de arbeidscontext anno 2018: enkele uitdagingen voor het rechtmatig verwerken van werknemersgegevens", *Arbeid. J.* 2017, 23-29; GDPR-eur, General Data Protection Regulation, https://gdpr-eu.be/wat-is-gdpr/, (consultatie 8 maart 2019); K. GIJSBRECHTS, "De GDPR wetgeving uitgelegd in vijf vragen", https://www.smartbiz.be/achtergrond/167961/de-gdpr-wetgeving-uitgelegd-vijf-vragen/, (consultatie 8 maart 2019).
[16] M. DE BACKER en T. FRANSEN, "Algemene Verordening Gegevensbescherming. Naar een nieuw concept inzake bescherming van persoonsgegevens?", *NJW* 2018, nr. 378, 190-203.
[17] GDPR-Eu, *General Data Protection Regulation,* https://gdpr-eu.be/wat-is-gdpr/, (consultatie 11 maart 2019).
[18] Art. 12, eerste lid GDPR; S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 212.
[19] Art. 13, tweede lid GDPR; GDPR-Eu, *General Data Protection Regulation,* https://gdpr-eu.be/wat-is-gdpr/, (consultatie 11 maart 2019).

gegevensverwerking". Dit beginsel houdt in dat enkel en alleen die gegevens worden verzameld, die noodzakelijk zijn om het begoode doel te bereiken.[20]

2.3.3 Rechtmatig en welbepaald doel

De verwerking van persoonsgegevens dient te steunen op één van de zes gronden opdat het rechtmatig zou zijn.[21] In tegenstelling tot de databeschermingsrichtlijn wordt het integriteits- en vertrouwelijkheidsbeginsel beschouwd als basisbeginsel. Dit zorgt ervoor dat elk onrechtmatig gebruik van persoonsgegevens moet worden voorkomen.[22]

Daarnaast moeten persoonsgegevens verkregen worden voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigde doeleinde. Echter stelt artikel 5, eerste lid van de GDPR dat een verwerking voor andere doeleinden dan die waarvoor de persoonsgegevens oorspronkelijk zijn verzameld wel mogelijk is, enkel als die verwerking verenigbaar is met die doeleinden. Deze doeleinden komen in grote lijnen overeen met de beginselen uit Richtlijn 95/46/EG, alleen is de verordening explicieter en krachtiger verwoord.

Bovendien moeten de persoonsgegevens worden bewaard in een vorm die het onmogelijk maakt de betrokkenen te identificeren langer dan noodzakelijk.[23] Een voorbeeld hiervan is het bijhouden van CV's van kandidaten langer dan noodzakelijk voor de doeleinden.

2.3.4 Toestemming

Persoonsgegevens zijn rechtmatig verwerkt mits er toestemming is gegeven door de betrokkenen. Deze dienen de toestemming te geven op een duidelijke en actieve manier, zoals bijvoorbeeld in een contract. Verder, is een mondelinge verklaring of het gebruik van elektronische middelen ook aanvaardbaar.[24]

De betrokkenen dienen vrij, geïnformeerd en duidelijk in te stemmen met het verwerken van hun persoonsgegevens. In dit geval, geldt het stilzwijgen van de betrokkenen niet als toestemming. Tevens geldt de toestemming voor alle verwerkingsactiviteiten die dezelfde doelen beogen. Bijgevolg, indien er verschillende doeleinden zijn, moet de toestemming telkens voor elk van de doeleinden worden toegekend. De bewijslast van de toestemming rust op de verwerkingsverantwoordelijke.[25]

Daarnaast geldt er voor het verwerken van persoonsgegevens van kinderen een specifieke bescherming, omdat zij minder bewust zijn over de gevolgen en risico's. Hierdoor is er een ouderlijke toestemming nodig bij het verwerken van de gegevens. De GDPR stelde een leeftijdsgrens op van 13 jaar.[26]

2.3.5 Persoonsgegevens

De GDPR heeft de term persoonsgegevens uitgebreid. Onder persoonsgegevens wordt het volgende verstaan *"alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon".*[27] Meer gegevens worden nu als persoonsgegevens beschouwd, waardoor de verwerking erg voorzichtig moet gebeuren.

---

[20] Art. 89 GDPR.
[21] Art. 6 GDPR.
[22] Art. 5, eerste lid, f) GDPR.
[23] Art. 5, eerste lid GDPR.
[24] S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 210.
[25] S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 212.
[26] Art. 7 GDPR.
[27] Art. 4 GDPR.

Een identificeerbaar natuurlijk persoon kwam ook aan bod in de databeschermingsrichtlijn, dus dit was geen nieuwigheid. Wel werd het begrip "identificeerbaar" verder uitgebreid. Krachtens overweging 30 van de GDPR worden indirecte gegevens zoals een IP-adres ook beschouwd als een identificeerbare gegeven.[28]

De categorie van bijzondere persoonsgegevens wordt naast de religieuze overtuigingen, politieke opvattingen en etnische afkomst ook verder uitgebreid met biometrische en genetische gegevens. Deze bijzondere gegevens krijgen ook een specifieke bescherming omdat ze grotere risico's kennen. Er geldt bijvoorbeeld een algemeen verbod op de verwerking van deze bijzondere gegevens, behoudens in de gevallen bepaald door de wet.[29]

Daarnaast is de GDPR niet van toepassing op anonieme gegevens, aangezien deze geen betrekking hebben op identificeerbare personen. Een voorbeeld hiervan zijn anonieme gegevens bij wetenschappelijke onderzoeken.[30]

2.3.6 Meer rechten voor natuurlijke personen

De GDPR heeft heel wat nieuwe rechten voorzien voor de betrokken natuurlijke personen. Het recht om vergeten te worden, recht op beperking van de verwerking en het recht op overdracht.[31]

2.3.6.1 Recht op vergetelheid

Alle betrokkenen hebben het recht om *"zonder onredelijke vertraging"* wissing van hun persoonsgegevens te verkrijgen van de verwerkingsverantwoordelijke. Deze is verplicht de gegevens te wissen in de volgende gevallen:

- De persoonsgegevens zijn niet langer vereist voor het doel waarvoor zij aanvankelijk zijn verzameld;
- De betrokken persoon trekt zijn toestemming in en er geen andere rechtsgrond is;
- De betrokken persoon maakt een bezwaar tegen de verwerking;
- De persoonsgegevens zijn onrechtmatig verwerkt;
- De persoonsgegevens moeten verwijderd worden om te voldoen aan een wettelijke verplichting van het Unierecht of lidstatelijk recht die op de verwerkingsverantwoordelijke berust;
- De persoonsgegevens zijn verzameld wegens een aanbod van diensten van de informatiemaatschappij aan kinderen.[32]

Belangrijk is dat dit recht niet absoluut is. Het moet afgewogen worden tegen de belangen van de verwerkingsverantwoordelijke.[33]

2.3.6.2 Recht op beperking van de verwerking

In bepaalde gevallen laat de GDPR toe om het gebruik van persoonsgegevens te beperken. In dat geval is de verwerker verplicht om *"zonder onnodige vertraging"* de verwerking te beperken. Indien de betrokkene zich op dit recht beroept, moet er wel één van de volgende elementen aanwezig zijn:

- Betwisting van de juistheid van de persoonsgegevens. Deze moeten dan door de verwerkingsverantwoordelijke gecontroleerd worden;
- De verwerking is onrechtmatig en de betrokkene verzoekt beperking van het gebruik;
- De persoonsgegevens zijn niet meer nodig, maar de betrokken heeft deze wel nodig om een claim te kunnen uitvoeren;

---

[28] Overweging 30 GDPR; M. DE BACKER en T. FRANSEN, "Algemene Verordening Gegevensbescherming. Naar een nieuw concept inzake bescherming van persoonsgegevens?", *NJW* 2018, nr. 378, 190-203.
[29] Art. 9, eerste lid GDPR.
[30] Art. 4, eerste lid GDPR; S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 210.
[31] S. ROYER en W. YPERMAN, "Horen, zien en (moeten) spreken: Grondwettelijk Hof vernietigt actieve meldplicht ocmw's" *DJK* 2019, nr. 386, 1-2.
[32] Art. 17, eerste lid GDPR.
[33] Art. 17, derde lid GDPR; X, "Uitzonderingen privacy-wet bij sociale inspectie", *DJK* 2015, nr. 307, 2.

- De betrokkene verzet zich tegen de verwerking. De verwerkingsverantwoordelijke is verplicht de verwerking stop te zetten, tenzij hij zwaardere dwingende gerechtvaardigde redenen aanhaalt.[34]

2.3.6.3 Recht op overdracht

Het recht van overdracht houdt in dat betrokkenen het recht hebben om hun persoonsgegevens bij de verwerkingsverantwoordelijke in een "*gestructureerde, gangbare en machineleesbare vorm*" te ontvangen. Daarnaast kunnen ze die laten overdragen aan een andere verwerkingsverantwoordelijke, in de gevallen waarin de verwerking berust op toestemming of op een overeenkomst of wanneer de verwerking via geautomatiseerde procedés wordt verricht.[35]

Het recht kan toegepast worden op digitale gegevens. Eveneens berust de verwerking op de toestemming van de betrokkenen, of op het opstellen van een overeenkomst met de betrokkenen. Tevens heeft een bedrijf de wettelijke verplichting om de betrokkenen te informeren over hun recht op overdracht.[36]

2.3.7 Verplichting tot betere beveiliging van persoonsgegevens

Onder de verordening gelden ook twee nieuwe verplichtingen, namelijk *privacy by design* en *privacy by default*. Ondernemingen moeten adequate maatregelen nemen om de verwerking van persoonsgegevens te beschermen.

Bij de ontwikkeling of de invoering van nieuwe systemen binnen een onderneming, moet er rekening worden gehouden met de privacy en de bescherming van persoonsgegevens. Er moeten verschillende beveiligingsmaatregelen genomen worden. Hoe gevoeliger de data, des te meer maatregelen een onderneming zal moeten nemen om schendingen te voorkomen.

2.3.7.1 Privacy by design

Privacy by design of gegevensbescherming door ontwerp houdt in dat bij het ontwikkelen van producten en diensten al rekening moet worden gehouden met privacy. Hierbij wordt dataminimalisatie gebruikt als uitgangspunt. Men moet zich met andere woorden afvragen of het verwerken van persoonsgegevens noodzakelijk is bij de ontwikkeling van desbetreffende producten en diensten. Een onderneming kan in dit geval opteren om met geanonimiseerde gegevens te werken.

Indien er toch persoonsgegevens worden verwerkt, moet de onderneming voor mogelijke beveiliging zorgen. Zo kan er gewerkt worden aan de hand van encryptie of pseudonimiseren. Deze worden wel nog gezien als persoonsgegevens, wat bij geanonimiseerde gegevens niet het geval is.[37]

2.3.7.2 Privacy by default

Privacy by default stelt dat organisaties verplicht zijn om de privacy van hun klanten te beschermen doordat zij een privacyvriendelijke stand gebruiken. Een voorbeeld hiervan is wanneer er iets besteld wordt op een website en onderaan staan de voorgeselecteerde vakjes met "Ik ga akkoord met …". *Privacy by default* zorgt ervoor dat de vakjes niet al voorgeselecteerd zijn, maar dat het aan de betrokkene is om dit actief te doen.[38]

2.3.8 Aanstelling DPO

De GDPR verplicht het aanstellen van een Data Protection Officer, hierna DPO. Helemaal nieuw is dit niet, want in de gegevensbeschermingsrichtlijn werd hier ook al naar verwezen. Echter was dit toen vrijblijvend.[39]

---

[34] Art. 18, eerste lid GDPR.
[35] Art. 20, eerste lid GDPR.
[36] Art. 20 GDPR.
[37] Art. 25 GDPR.
[38] Art. 25 GDPR.
[39] J.F. HENROTTE en F. COTON, "Everything you always wanted to know about DPO (but were afraid to ask)", *CDJ* 2017, nr. 2, 32-42.

De rol van de DPO wordt in de GDPR verder ingevuld. Deze heeft een adviserende, informerende en controlerende functie over gegevensbescherming. De DPO zorgt ervoor dat het bedrijf de regels van de GDPR naleeft. Verder staat een DPO in voor het creëren van privacy awareness binnen het bedrijf en het verzamelen van informatie om verwerkingsactiviteiten te identificeren.[40]

De DPO kan een werknemer zijn binnen de onderneming en zal aangewezen worden op basis van zijn kwaliteiten en expertise op het vlak van gegevensbescherming. Daarnaast zal hij ook de contactpersoons zijn naar verschillende partijen toe. Zo is hij de contactpersoon voor de betrokkene, maar ook voor de overheid en Gegevensbeschermingsautoriteit.[41]

De GDPR verplicht het benoemen van een DPO als:

- De verwerking wordt uitgevoerd door een overheid;
- Bedrijven die hoofdzakelijk belast zijn met verwerkingen die vanwege hun aard, omgang en of doelen regelmatige en systematische observatie op grote schaal van betrokkenen eisen;
- Bedrijven die belast zijn met grootschalige verwerking van bijzondere categorieën persoonsgegevens.[42]

2.3.9 De toezichthoudende autoriteit

Ten einde de bescherming van de persoonsgegevens te verzekeren, kreeg de toezichthoudende autoriteit een centrale rol bij de niet-naleving van de GDPR. Hierdoor werd de privacycommissie gemoderniseerd en wordt eerder een "waakhond" die naast een adviserende functie ook een sanctionerende functie kreeg. Hierbij verdween de Belgische Privacycommissie en werd vanaf 25 mei 2018 vervangen door de Gegevensbeschermingsautoriteit, hierna GBA.[43]

Zowel ondernemingen als natuurlijke personen kunnen een klacht indienen bij de GBA, indien er niet correct wordt omgegaan met persoonsgegevens. Deze klacht wordt onderzocht en kan gesanctioneerd worden met een geldboete.[44] Het opleggen van administratieve geldboetes heeft als doel om de naleving van de GDPR te verzekeren en afschrikkend te werken. Tevens moeten deze ook evenredig zijn, waardoor de hoogte van een geldboete kan verschillen naargelang de situatie.[45] De geldboete kan 4% van de wereldwijde omzet bedragen of 20 miljoen euro bedragen voor inbreuken op essentiële bepalingen, bijvoobeeld het niet naleven van de voorwaarden rond toestemming. Daarnaast is er ook een sanctie voorzien van 2% van de wereldwijde omzet of 10 miljoen euro voor bijvoorbeeld het niet melden van een data-breach.[46]

De toezichthoudende autoriteit houdt rekening met verschillende elementen bij het opleggen van een geldboete. Er wordt bijvoorbeeld gekeken naar de aard en de ernst van de inbreuk en of het met opzet is gebeurd. Ook de categorieën van persoonsgegevens spelen een rol.[47]

---

[40] Art. 39, eerste lid GDPR; E. JACOBS, "Acht misverstanden over nieuwe Europese privacyverordening, *DJK* 2017, nr. 345, 13.
[41] Art. 37, tweede en vijfde lid GDPR.
[42] Art. 37, eerste lid GDPR; S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 220.
[43] T. BALTHAZAR, "Privacycommissie wordt Gegevensbeschermingsautoriteit", *DJK* 2018, nr. 362, 2.
[44] Art. 58, eerste lid, i) GDPR.
[45] Art. 83, eerste lid GDPR.
[46] M. DE BACKER en T. FRANSEN, "Algemene Verordening Gegevensbescherming. Naar een nieuw concept inzake bescherming van persoonsgegevens?", *NJW* 2018, nr. 378, 190-203.
[47] Art. 83, tweede lid GDPR.

3 Privacy awareness

3.1 Pivacy

De definitie van privacy gaat ver terug in de tijd. Juridisch gezien werd privacy voor het eerst genoemd door Louis Brandeis en Samuel Warren. Brandeis en Warren waren twee advocaten die in 1890 privacy omschreven als het recht van een persoon "To be left alone" oftewel het recht om met rust gelaten te worden. Privacy wordt gezien als een sociaal gegeven, dat afhangt van maatschappelijke, culturele en situationele parameters en kan simpelweg niet worden gedefinieerd.[48]

Door de bloei van de informatica in de jaren 70, begon men met de automatische verwerking van persoonsgegevens. Door deze nieuwigheid begon met na te denken over de mogelijke risico's voor de persoonlijke levenssfeer van de burgers. Dit resulteerde uiteindelijk in verschillende internationale basisbeginselen. In 1992 ontstond ook onze nationale privacywetgeving.[49]

Doordat privacy zo gevoelig is voor maatschappelijke veranderingen, is de Europese Unie tegemoetgekomen aan de verschillende technologische evoluties door middel van de GDPR. Hiermee werd haar voorgaande privacyrichtlijn aangepast aan onze huidige samenleving. Bovendien is privacy een grondrecht dat op verschillende niveaus wordt geregeld, zowel op nationaal als op Europees niveau.[50]

3.1.1 Historiek

Alvorens de Belgische privacywetgeving uiteen te zetten, is het belangrijk om artikel 8 van het Europees Verdrag voor de rechten van de mens (EVRM) te benadrukken. Dit artikel benadrukt onder andere de eerbiediging voor het privéleven.[51] Daarnaast is het huidige artikel 22 in onze grondwet opgebouwd in het licht van artikel 8 van het EVRM. Artikel 22 van het grondwet stelt dat iedereen het recht heeft op de eerbiediging van zijn privé-leven en zijn gezinsleven, behoudens in de gevallen bepaald door de wet.[52]

In België werd de privacybescherming geregeld door de wet tot bescherming van de persoonlijke levenssfeer, ook de Privacywet genoemd.[53] Deze wet was gebaseerd op het Vedrag van de Raad van Europa voor de bescherming van individuen met betrekking tot de automatische verwerking van persoonlijke gegevens.

De Privacywet benadrukte twee beginselen, namelijk het finaliteitsbeginsel en het proportionaliteitsbeginsel. Het finaliteitsbeginsel bepaalt dat persoonsgegevens enkel verwerkt moge worden in specifieke gevallen. Het proportionaliteitsbeginsel geeft aan dat de verzamelde en verwerkte persoonsgegevens noodzakelijk en relevant moeten zijn.[54]

In 1971 werd reeds een wetsvoorstel ingediend met betrekking tot de bescherming van persoonsgegevens. Hierrond werd in 1976 het eerste wetsontwerp ingediend, maar dit heeft echter nooit tot nationale wetgeving geleid. Desondanks de mislukking van deze poging, kwam er wel een aantal wetten tot stand. Echter bleven deze beperkt tot de organisatie van de reeds bestaande databanken. Denk hierbij aan de Rijksregisterwet van 8 augustus 1983 die het Rijksregister trachtte te

---

[48] M. OTTO, *The Right to Privacy in Employment: A comparative Analysis*, Oxford, Hart Publishing, 2016, 256; F. HENDRICKX, "Privacy en arbeidsrecht", *Jura Falc.* 1998-1999, nr. 4, 619-642.
[49] M. FRIEDEWALD en R.J. POHORYLES, *Privacy and Security in the Digital Age*, Oxon, Routledge, 2016, 212.
[50] A. VEDDER en Y. VAN DER SYPE, "Privacy, werk en internet of things", *ORM* 2016, nr. 5, 118-127.
[51] Art. 8 EVRM.
[52] Art. 22 Gw.
[53] Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993.
[54] Art. 4, eerste lid Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993.

regulariseren. Dit was natuurlijk een belangrijke stap, aangezien het Rijksregister informatie bevatte van alle Belgen.[55] Deze wet bepaalde de manier waarop die gegevens werden bijgewerkt, bewaar en beheerd.[56]

Er was toen geen gebrek aan wetgevende intiatieven, echter resulteerde dit nooit in het gewenste resultaat.

In 1995 wordt er door het Europees parlement en de Raad de richtlijn 95/46/EG betreffende de bescherming van de natuurlijke persoon in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, goedgekeurd. Het was te merken dat Europa de regels betreffende de bescherming van persoonsgegevens gelijk wou stellen binnen de Europese Unie.[57] Deze richtlijn verplichtte alle lidstaten tot de aanpassing van hun privacywetgeving. In België werd deze richtlijn in 1998 omgezet in een wet. Dit werd ook de eerste aanpassing van de wet van 1992. De verschillen waren te merken in bepaalde aspecten zoals het recht om zich te verzetten, de regeling voor bijizondere gegevens en de mogelijkheid om een verantwoordelijke aan te stellen.[58]

De bescherming van de persoonsgegevens werd in 2000 ook opgenomen in het Handvest van de Grondrechten van de Europese Unie. Krachtens artikel 8 van dit Handvest heeft *"eenieder het recht op bescherming van de hem betreffende persoonsgegevens."*[59]

De laatste wijziging van de privacywet gebeurde met de voorstelling van de GDPR. Op 25 januari 2012 kwam de Europese Commissie met een voorstel tot een nieuw Europees privacyrecht. Het doel was een grondige actualisering van de Europese richlijn van 1995. Bovendien werden er onder andere volgende wijzigngen vooropgesteld: De verwerkers van persoonsgegevens zouden meer verantwoordelijkheid en rekenschap krijgen. Er moet slechts één nationale gegevensbeschermingsautoriteit zijn. Burgers kunnen gemakkelijker toegang krijgen tot hun gegevens. Een recht om vergeten te worden zal mogelijk zijn.[60]

Dit voorstel werd na intensieve debatten op 8 april 2016 goedgekeurd, en zoals hierboven vermeld, op 25 mei 2018 ingetreden.

3.2 Awareness van de werknemers

Organisaties hebben ondertussen een uitgeschreven privacy policy die je kan vinden op hun websites, een verwerkingsregister opgezet om hun activiteiten in kaart te brengen, verwerkersovereenkomsten gesloten met verwerkers,… Kortom heel wat tijd en moeite gestoken in informatiebeveiliging sinds en voor de intreding van de GDPR één jaar geleden. De vraag is in welke mate zijn de werknemers op de hoogte? En hoe zorg je ervoor als organisatie dat de werknemers bewust blijven?[61]

---

[55] P. DE HERT en S. GUTWIRTH, *Anthologie privacy overzicht van artikels wetgeving en rechtsspraak over privacy- en persoonsgegevensbescherming voor België tot 1998,* Brussel, ASP, 2013, 19-20.
[56] Wet 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *BS* 21 april 1984.
[57] Richtl. EP & Raad nr. 281/31, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de veverwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *PB.L.* 23 november 1995.
[58] Art. 2, 9 en 14 Wet 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de veverwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *BS* 2 maart 1999.
[59] Art. 8 Handvest van de Grondrechten van de Europese Unie.
[60] Gegevensbeschermingsautoriteit, "Nieuwe privacywetgeving (AVG), https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-0, (consultatie 31 mei 2019).
[61] I. HUIS, "Meten is weten: hoe doe je dat met privacy awareness?", https://www.privacycompany.eu/meten-is-weten-hoe-doe-je-dat-met-privacy-awareness/, (consultatie 29 mei 2019).

Het is van belang dat sleutelfiguren binnen organisaties goed op de hoogte zijn van de GDPR. Awareness of bewustwording moet worden gecreëerd onder de werknemers. Privacy moet niet alleen in het beleid staan, maar moet ook terug te vinden zijn in de cultuur, in de dagelijkse gedachten van de werknemers en met dit probleem kampen heel wat organisaties.[62]

Het aanpakken van het kennisniveau is een belangrijke eerste stap. Dit zal de werknemers een algemeen beeld van privacy en een inzicht in de mogelijke risico's geven, voor zowel de klanten als voor zichzelf. Het ontbreken van privacy awareness binnen organisaties brengt ook met zich mee dat er een verhoogd risico is op het krijgen van een boete.[63]

Daarnaast is het van belang dat werknemers weten dat de GDPR ook voor hen van toepassing is en niet alleen voor de klanten, dat die bescherming ook voor hen als werknemers geldt en dat ze die rechten kunnen toepassen.

Om ervoor te zorgen dat er awareness is onder de werknemers, is het belangrijk dat zij de nodige kennis krijgen op het gebied van privacy. Werknemers moeten getraind worden in het herkennen van privacygevoelige kwesties. Ze dienen ook te weten welke acties ze moeten ondernemen in geval van een datalek en hoe zij op een correcte wijze persoonsgegevens moeten verwerken.[64]

3.3 Privacy training binnen Ordina

Binnen Ordina is een e-learning beschikbaar voor iedere nieuwe werknemer. De deelname aan de e-learning is verplicht. De e-learning is een 100% online cursus en gaat in op wat privacy is en wat de werknemers kunnen doen om op een veilige en voorzichtige manier met persoonsgegevens om te gaan. Op het einde van de e-learning is er een quiz met een aantal vragen over de geziene informatie.

[62] A. KEEREMAN, "Privacybescherming werknemers in wiskundige formule (interview met Yung Shin Van Der Sype)", *DJK* 2017, nr. 352, 5; RIS-Rijkschroeff Juristen, "De algemene Verordening Gegevensbescherming en awareness", https://www.ris-rijkschroeff.nl/Privacyrecht/De-Algemene-Verordening-Gegevensbescherming-en-awareness, (consultatie 28 mei 2019).

[63] R. SAELENS en P. DE HERT, "Raad voor Vreemdelingenbetwisting – Elektronische procesvoering – Privéleven – Bescherming persoonsgegevens – Informatieveiligheid – Bescherming communicatiegeheim", *RW* 2016-17, nr. 15, 584-588.

[64] RIS-Rijkschroeff Juristen, "De algemene Verordening Gegevensbescherming en awareness", https://www.ris-rijkschroeff.nl/Privacyrecht/De-Algemene-Verordening-Gegevensbescherming-en-awareness, (consultatie 28 mei 2019).

4 Arbeidscontext

Privacy is een maatschappelijk gegeven waar niemand omheen kan. Dit geldt ook voor de arbeidsverhouding. We kennen reeds de strenge privacybescherming waaraan werkgevers zich moeten houden, zoals het recht op eerbiediging van het privéleven, erkend door zowel artikel 8 van het EVRM als door artikel 22 van onze Grondwet. Er mag niet afgeweken worden van dit recht gedurende de volledige duur van de arbeidsovereenkomst. Het recht op privacy van werknemers is duidelijk aan de orde.

Echter is de context van de arbeidsrelatie wat complex. Er botsen namelijk twee principes met elkaar: het gezag van de werkgever en het recht op eerbiediging van het privéleven van de werknemers.[65]

4.1 Het gezag van de werkgever

Er wordt aangenomen dat bij het aangaan van een arbeidsrelatie, de werknemer impliciet toestemt met een zekere beperking van zijn fundamentele grondrechten, zoals zijn recht op privacy. Deze ondergeschikte relatie tussen de werkgever en de werknemer veronderstelt namelijk steeds een zekere mate van inmenging door de werkgever bij de uitoefening van zijn gezag en controlerecht.[66]

Het feit dat de werknemer een arbeidsovereenkomst afsluit, geeft aan dat hij akkoord gaat met het uitvoeren van activiteiten in naam en voor rekening van zijn werkgever en bijgevolg instemt met een aantal beperkingen op de uitoefening van zijn basisrecht op privacy.

4.2 Het recht op eerbiediging van het privéleven van de werknemers

In theorie genieten werknemers van een uitgebreide bescherming op hun privéleven en van hun persoonsgegevens. Deze bescherming wordt op verschillende wijzen en niveaus gewaarborgd. Enerzijds genieten zij de bescherming die voor elk individu geldt en anderzijds genieten zij van specifieke beschermingsmechanismen die enkel op werknemers van toepassing zijn.[67]

Wat betreft de algemene bescherming van het recht op privacy die elk individu geniet, zijn artikel 8 van het EVRM en de GDPR voornamelijk van belang. Naast deze algemene bescherming, is ook een bijzondere bescherming uit de specifieke regelgeving omtrent de bescherming van hun persoonlijke levenssfeer binnen de onderneming. Zo voorzien verscheiden collectieve arbeidsovereenkomsten bescherming. Voor wat betreft de elektronische controle van de arbeid, wordt de bescherming geregeld in CAO nr. 81.[68]

Kortom genieten werknemers naast de privacybescherming die ze genieten als individu en gegevensbescherming als betrokkene, genieten zij ook van specifieke beschermingsregimes als werknemers binnen een onderneming.[69]

Ondanks de veelheid aan juridische bronnen, zijn er toch een aantal beperkingen op de privacybescherming van werknemers in de praktijk. Er moet namelijk rekening worden gehouden met de rechten en belangen van anderen. Dit bevestigd de niet-absolute karakter van de privacynormen.[70]

4.3 Persoonsgegevens binnen de arbeidscontext

Voor de toepassing van de verordening wordt een verwerking beschouwd als een bewerking met betrekking tot persoonsgegevens, onder andere het verzamelen, opvragen, wijzigen en wissen van gegevens. Hieronder vallen ook

---

[65] F. HENDRICKX, "Privacy en arbeidsrecht", *Jura Falc.* 1998-1999, nr. 4, 619-642.
[66] A. VEDDER en Y. VAN DER SYPE, "Privacy, werk en internet of things", *ORM* 2016, nr. 5, 121; F. HENDRICKS, *Privacy en arbeidsrecht*, Brugge, die Keure, 1999, 47.
[67] A. VEDDER en Y. VAN DER SYPE, "Privacy, werk en internet of things", *ORM* 2016, nr. 5, 118-120.
[68] Y. VAN DER SYPE, "Een geïntegreerde methode voor de beoordeling van de privacy- en persoonsgegevensbescherming van werknemers", *SK* 2017, nr. 10, 377-398.
[69] A. VEDDER en Y. VAN DER SYPE, "Privacy, werk en internet of things", *ORM* 2016, nr. 5, 121
[70] Y. VAN DER SYPE, "Een geïntegreerde methode voor de beoordeling van de privacy- en persoonsgegevensbescherming van werknemers", *SK* 2017, nr. 10, 377-398.

verwerkingen van persoonsgegevens van werknemers in het kader van de loonadministratie. Deze definitie is aldus zeer ruim.[71]

De GDPR spreekt over persoonsgegevens die direct of indirect een persoon identificeren. Als voorbeeld binnen de arbeidsrelatie kunnen volgende gegevens vermeld worden: naam, adres, rekeningnummer, ID-nummers van werknemers, de werkroosters en de personeelsdossiers. De verwerking van deze gegevens dient te steunen op een Rechtmatige grond, waarbij de verwerking toelaatbaar is. Bijgevolg kunnen werknemersgegevens rechtmatig worden verwerkt, indien de werkgever wettelijk verplicht wordt tot een verwerking, de verwerking noodzakelijk is voor de uitvoering van de arbeidsovereenkomst of in geval dat de verwerking noodzakelijk is voor het vervullen van gerechtvaardigde belangen van de werkgever of van derden.[72] Zo kan een werkgever bij het verwerken van loongegevens van zijn werknemer in het kader van een salarisstudie steunen op zijn eigen gerechtvaardigd belang om kennis te krijgen van de resultaten.

In mindere mate, leidt de toestemming van de werknemer ook tot een rechtmatige verwerking. Hoewel deze toestemming niet wordt uitgesloten door de verordening, is deze toch een iets zwakke juridische grond voor de verwerking. Krachtens considerans 34 van het voorstel van 2012, werd de toestemming uitgesloten als geldige rechtsgrondslag voor de verwerking wanneer er een onevenwichtigheid is tussen de positie van de betrokkenen en die van de verwerkingsverantwoordelijke.[73] Dit gebeurt wanneer werknemersgegevens worden verwerkt door de werkgever in het kader van de arbeidsrelatie. Het vrije karakter van de toestemming staat immers steeds onder druk binnen de arbeidscontext. Dit komt door de ondergeschikte positie van de werknemer ten opzichte van zijn werkgever.[74] De GDPR behoudt met andere woorden de toestemming als rechtsgrond, maar legt er wel striktere voorwaarden aan op. [75]

Voor de verwerking van bijzondere persoonsgegevens, zijn de toelaatbaarheidsvoorwaarden strikter. Dit zijn persoonsgegevens waaruit volgende informatie uitgehaald kan worden: de etnische afkomst, politieke opvattingen, religieuze overtuigingen of het lidmaatschap van een vakbond. De verwerking is in beginsel verboden. Echter is het verwerken van deze bijzondere categorie van persoonsgegevens toegelaten in bepaalde omstandigheden, namelijk wanneer de verwerking noodzakelijk is binnen de arbeidsrelatie, de verwerking noodzakelijk is voor een rechtsvordering of voor bepaalde preventieve doeleinden.[76]

4.4 Betere beveiliging van persoonsgegevens

Door de snelle technologische vooruitgang tijdens de laatste decennia zijn ondernemingen verplicht sterkere beveiligingsmaatregelen te nemen. Volgens de GDPR is het verstandig voor ondernemingen om hun gegevensbeschermingsbeleid methodisch aan te pakken. Om te beginnen moet de werkgever een risicoanalyse uitvoeren en op basis daarvan worden bijpassende maatregelen genomen.[77]

Binnen de GDPR wordt deze risicoanalyse bestempeld als een gegevensbeschermingseffectbeoordeling of data protection impact assessment, hierna DPIA. Een DPIA is met andere woorden een beoordeling die wordt uitgevoerd door de verwerkingsverantwoordelijke alvorens de persoonsgegevens worden verwerkt. Vervolgens wordt er gekeken naar de mogelijke risico's in verband met de rechten en vrijheden van de betrokkene. Indien uit deze DPIA risico's blijken te zijn,

---

[71] S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 211.
[72] Art. 6 GDPR.
[73] Art. 7 GDPR juncto considerans 34 van het voorstel van 2012.
[74] Y.S., VAN DER SYPE, "Bescherming van persoonsgegevens in de arbeidscontext anno 2018: enkele uitdagingen voor het rechtmatig verwerken van werknemersgegevens", *Arbeid. J.* 2017, 23-29; Art. 29 werkgroep, "Opinie 2/2017 on data processing at work", *WP* 249, 2017, 6.
[75] S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 212.
[76] Art. 9-10 GDPR; S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 213.
[77] Y. VAN DER SYPE, "De gegevensbeschermingseffectbeoordeling voor de verwerking van werknemersgegevens", *ORM* 2018, nr. 1, 2-11.

dient er gekeken te worden naar de beste manier om deze te beheersen. Hierbij moeten passende maatregelen genomen worden opdat de rechten en vrijheden van de betrokkene beschermd worden.[78]

Bovendien dient de verwerkingsverantwoordelijke ingeval van een hoog risico bij gebrek aan maatregelen, de Gegevensbeschermingsautoriteit voorafgaand aan de verwerking om advies te vragen.[79]

4.5 De informatieplicht tegenover de werknemers

Hoewel de informatieplicht tegenover de werknemers reeds bestond, is deze onder de GDPR wetgeving uitgebreid. De informatieplicht houdt immers in dat de werkgever de nodige inlichtingen beschikbaar stelt aan de werknemer, wanneer hij zijn persoonsgegevens verwerkt. In eerste instantie dient de werkgever de inlichtingen te geven ten laatste op het moment waarop de persoonsgegevens verkregen zijn.[80] In tweede instantie kan hij de informatie beschikbaar stellen uiterlijk binnen één maand na het verkrijgen van de gegevens.[81]

Zo moeten werknemers weten voor welke doeleinden hun gegevens worden verwerkt, welke categorie van gegevens verwerkt worden, waar hij de gegevens vandaan haalt en aan wie de gegevens worden meegedeeld. Verder is het ook van belang om mee te delen bij wie de werknemers zich kunnen wenden om hun rechten uit te oefenen en moeten zij duidelijk geïnformeerd worden over de voorziene rechten. Bovendien moet de werkgever ook aangeven op welke rechtsgrond hij de verwerking baseert. Persoonsgegevens van werknemers worden in de arbeidscontext vaak verwerkt omdat dit binnen de gerechtvaardigde belangen van de werkgever valt. Nu verplicht de GDPR de werkgever om ook dit gerechtvaardigd belang te omschrijven. [82]

Bovendien is het volgens de GDPR ook noodzakelijk om de werknemer te informeren over de periode gedurende welke gegevens opgeslagen zullen worden en dat de betrokkene het recht heeft zijn toestemming op ieder moment in te trekken. Daarnaast moet het recht om een klacht in te dienen bij de toezichthoudende autoriteit meegedeeld worden.[83]

4.5.1 Rechten van de werknemer

De werkgever moet zijn werknemers informeren over de verschillende rechten ten opzichte van de verwerking van hun persoonsgegevens.

Het **recht van inzage en kopie** houdt in dat de betrokkenen het recht hebben om allerlei vragen te stellen in verband met het verwerken van hun gegevens. Bijvoorbeeld de reden van de verwerking, waar de gegevens gehaald worden, wie over de gegevens beschikt, hoe lang de gegevens bewaard worden en of de gegevens naar een land buiten Europa worden verstuurd. Daarnaast is een inzage van de gegevens mogelijk zonder hiervoor een reden te geven. Het is dus aan de verwerkingsverantwoordelijke om maatregelen te nemen opdat de informatie op een transparante, duidelijke en toegankelijke manier kan worden verstrekt.[84]

De werknemers hebben bovendien het **recht om een verbetering** te bekomen van alle onjuiste informatie.[85] Eveneens kan er gevraagd worden om alle persoonsgegevens te laten **wissen** en niet verder te laten verwerken, wanneer de persoonsgegevens niet langer noodzakelijk zijn voor het doeleinde waarvoor zij oorspronkelijk werden verzameld. Het recht

---

[78] Art. 35, eerste lid GDPR.
[79] S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 221; A. KEEREMAN, "Privacybescherming werknemers in wiskundige formule (interview met Yung Shin Van Der Sype)", *DJK* 2017, nr. 352, 5.
[80] Art. 13 GDPR.
[81] Art. 14, derde lid GDPR.
[82] S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 218.
[83] Art. 12, vierde lid GDPR.
[84] Art. 15, eerste lid GDPR; S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 215.
[85] Art. 16 GDPR; S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 216.

op wissen is eveneens mogelijk wanneer de betrokkenen hun toestemming intrekken en er geen andere rechtsgrond bestaat voor de verwerking, of wanneer de persoonsgegevens op een onrechtmatige wijze werden verwerkt.[86]

De GDPR voorziet ook een **recht van bezwaar** voor de werknemers. Bijgevolg moet de werkgever de verwerking stopzetten, tenzij er een gegronde reden is. Betrokkenen waarvan de persoonsgegevens verwerkt worden ten behoeve van direct marketing, hebben te allen tijde het recht van bezwaar in te schakelen. Echter kan geen bezwaar plaatsvinden wanneer de verwerking van de persoonsgegevens op dwingende gronden steunt, die zwaarder wegen dan de rechten en vrijheden van de werknemer. Een voorbeeld hiervan is wanneer de verwerking noodzakelijk is voor de uitvoering van een arbeidsovereenkomst, of wanneer de verwerking gebaseerd is op een verplichting waar de verwerkingsverantwoordelijke aan onderworpen is.[87]

De werknemers beschikken ook over een **recht op beperking** van de verwerking van persoonsgegevens in volgende gevallen: wanneer de gegevens onjuist zijn, wanneer de verwerking onrechtmatig is of wanneer de verwerkingsverantwoordelijke de persoonsgegevens niet meer nodig heeft, maar deze nog wel nodig zijn door de betrokkene voor de instelling, uitoefening of onderbouwing van een rechtsvordering.[88] Dit moet duidelijk in het bestand worden aangegeven. Hierdoor kan de werkgever slechts persoonsgegevens van zijn werknemer verwerken als deze laatste zijn toestemming geeft, in geval van een rechtsvordering of ter bescherming van de rechten van anderen.[89]

Tenslotte hebben werknemers immers het **recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking** zoals bij sollicitaties via internet zonder menselijke tussenkomst.[90] De reglementering voorziet de volgende uitzonderingen:

- Als het noodzakelijk is voor de arbeidsovereenkomst;
- Als het toegelaten is door nationale regelgeving;
- Als werknemer uitdrukkelijk zijn toestemming geeft.[91]

4.5.2 Tijdstip van informatieplicht

De werkgever moet zijn werknemers informeren ten laatste op het ogenblik van de verzameling van de persoonsgegevens. De werknemers hoeven niet meer geïnformeerd te worden als ze dit reeds wisten.[92]

In de gevallen waarbij de werkgever de persoonsgegevens niet bij de werknemers zelf verzamelt maar elders, moet dit ook aan de werknemers meegedeeld worden. Hiervan mag afgeweken worden wanneer het meedelen van de informatie onmogelijk blijkt of immens veel inspanning zou vergen, het verkrijgen van de gegevens wettelijk is of wanneer de persoonsgegevens vertrouwelijk moeten blijven.[93]

Er wordt ook ten sterkste aangeraden om de werknemers bij het begin van de arbeidsovereenkomst te informeren over de mogelijke verwerking van hun persoonsgegevens en al hun rechten hieromtrent.

4.5.3 Wijze van informatieplicht

De informatieplicht over de verwerking is niet gebonden aan vormvoorwaarden. Toch wordt er aangeraden om de kennisgeving schriftelijk te doen. De werkgever moet kunnen bewijzen dat zijn werknemers concreet en juist werden geïnformeerd. De manier waarop hij dit doet, heeft geen belang. Echter moet hij ervoor zorgen dat de werknemers niet zelf

---

[86] Art. 17 GDPR; S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 216.
[87] Art. 21 GDPR.
[88] Art. 18, eerste lid GDPR, S. RAETS, "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 217.
[89] Art. 18, tweede lid GDPR.
[90] G. VANDERSTICHELE, "Rechtspraak in een datagestuurde informatiemaatschappij", *NJW* 2017, nr. 368, 618-635.
[91] Art. 22 GDPR.
[92] Art. 13 GDPR.
[93] Art. 14 GDPR.

moeten zoeken naar de informatie, maar dat het actief door hem gebeurt, bijvoorbeeld met workshops, e-learnings, filmpjes enzovoort.

In het kader van de arbeidsrelatie kan de kennisgeving worden toegevoegd aan het arbeidsreglement, ofwel individueel worden getekend door de werknemers. Daarnaast kan de kennisgeving steeds aangepast worden aan nieuwe situaties.

Wat betreft het taalgebruik wordt een lange onduidelijke tekst afgeraden. De gebruikte taal moet gemakkelijk te begrijpen zijn en aangepast aan het doelpubliek. Vage bewoording moet vermeden worden.

Met deze voorwaarden kan er rekening worden gehouden bij het opstellen van de privacy policy.[94]

4.6 Datalek

Vele denken dat een datalek beperkt is tot het hacken van een computer. Maar niets is minder waar. Datalekken bestaan namelijk wanneer er inbreuken zijn op de beveiliging die zowel per ongeluk als op onrechtmatige wijze leiden tot vernietiging, verlies of verstrekking van de ongeoorloofde toegang tot persoonsgegevens.[95] Het gaat dus niet enkel om de gevallen waarbij hackers persoonsgegevens proberen te bemachtigen. Bijgevolg, voorziet de GDPR bijkomende verplichtingen wanneer het gaat om datalekken van persoonsgegevens.[96]

De verwerkingsverantwoordelijke is belast met het documenteren van alle inbreuken in verband met persoonsgegevens. Naast de feiten over de inbreuk, zal hij ook de gevolgen ervan en de genomen maatregelen moeten beschrijven. In de gevallen waarbij een gegevenslek een hoog risico kan vormen voor de rechten en vrijheden van de betrokkenen, moet de verwerkingsverantwoordelijke dit zo snel mogelijk meedelen aan zowel de Gegevensbeschermingsautoriteit als de betrokkenen. Krachtens artikel 33 is de verwerkingsverantwoordelijke verplicht om de inbreuk te *melden "zonder onredelijke vertraging en uiterlijk 72uur nadat hij er kennis van heeft genomen"* aan de Gegevensbeschermingsautoriteit.[97] In de arbeidsrelatie moet de werkgever in duidelijke en eenvoudige taal het gegevenslek aan de betrokken werknemer omschrijven.[98]

De GDPR beschrijft echter enkele uitzonderingen op deze mededelingsplicht. Deze is immers niet verplicht wanneer één van de onderstaande voorwaarden is vervuld:

- Wanneer de werkgever reeds passende technische en organisatorische beschermingsmaatregelen heeft genomen en deze zijn toegepast op de getroffen persoonsgegevens;
- Wanneer de werkgever achteraf maatregelen heeft genomen om te vermijden dat het hoge risico zich opnieuw voordoet;
- Wanneer de mededeling voor onevenredige inspanningen zou zorgen. In dit geval komt er een openbaar bericht in de plaats.[99]

Een meldplicht aan de bevoegde autoriteit geldt wanneer er sprake is van een risico voor de rechten en vrijheden van de betrokkenen. Bovendien heerst ook een verplichting om het datalek mee te delen aan de betrokkene, indien hij of zij een hoog risico lopen.

De meldplicht rust op de verwerkingsverantwoordelijke of op de verwerker indien de verwerkingsverantwoordelijke hierover schriftelijke afspraken heeft gemaakt met de verwerker. De melding zorgt ervoor dat de autoriteit het risico van het gegevenslek kan inschatten en zo aanbevelingen geven over het minimaliseren van het risico voor de betrokkene. Daarnaast

---

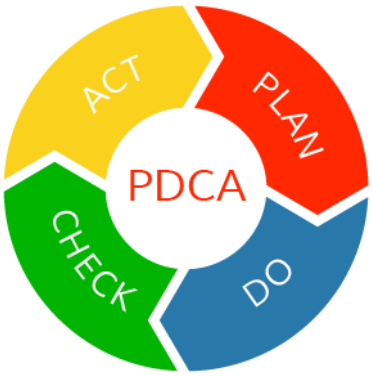
[94] Working Group 29, guidelines on transparency under Regulation 2016/679, 17/EN, 7-8.
[95] Working Group 29, Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens, 18/NL, 7.
[96] T. VAN GREMBERGHE, "GDPR legt procedure vast bij datalekken", *De Juristenkrant* 2017, nr. 358, 7.
[97] Art. 33, eerste lid GDPR.
[98] Art. 34, tweede lid GDPR; Working Group 29, Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens, 18/NL, 26.
[99] Art. 34, derde lid GDPR; T. VAN GREMBERGHE, "GDPR legt procedure vast bij datalekken", *De Juristenkrant* 2017, nr. 358, 7.

wordt de verantwoordelijke verplicht om na te denken over de manier waarop de gegevensverwerking wordt georganiseerd en beveiligd.[100]

[100] T. VAN GREMBERGHE, "GDPR legt procedure vast bij datalekken", *De Juristenkrant* 2017, nr. 358, 7.

5 Onderzoek binnen Ordina

De ideale situatie binnen Ordina en binnen elk ander bedrijf zou zijn dat alle werknemers preventief en zorgvuldig omgaan met persoonsgegevens. Opdat dit van toepassing zou zijn, moet iedereen goed op de hoogte zijn en simpelweg privacy bewust zijn. Daarnaast, trachten we te weten te komen of dat werknemers weten dat de bescherming van de GDPR ook op hen van toepassing is, en niet alleen op hun klanten.



Figuur 1: Plan-Do-Check-Act model

5.1 Plan

Het doel van mijn onderzoek is om privacy awareness te creëren bij de werknemers van Ordina rondom de GDPR en binnen de arbeidscontext. Als eerst ben ik begonnen met het opstellen van een plan van aanpak en dacht na over al mijn onderzoeksvragen, zoals is er een gebrek aan privacy bewustzijn binnen Ordina? Worden de werknemers goed op de hoogte gebracht van hun eigen rechten? Hoe pakt Ordina het privacy bewustzijn aan? En heeft die aanpak degelijk effect?

Naast het brainstormen over de probleemstelling, heb ik tijdens mijn planfase ook nagedacht over oplossingen. Wat direct naar voor kwam in gesprek met mijn mentor en Data Protection Officer was om op het einde van mijn stage een campagne te houden, waarbij ik een presentatie rond privacy awareness zou houden voor mijn doelpubliek.

5.2 Do

De tweede fase stond in het teken van het verzamelen van informatie. Het nam veel tijd in beslag om de GDPR te onderzoeken en te analyseren. Het is namelijk een zeer ruim onderwerp. Door het raadplegen van verschillende informatiebronnen en alle kennis die ik gedurende mijn stage meekreeg, lukte het me om een hoop informatie te verzamelen. Vervolgens heb ik deze informatie kritisch verwerkt om de GDPR binnen de arbeidscontext te begrijpen.

Daarnaast heb ik besloten om de kennis van de werknemers te toetsen op basis van een bevraging. Deze werd opgesteld uit GDPR-gebaseerde vragen in de vorm van scenario's.

5.3 Check

Na overleg met mijn docent, werd er besloten dat ik de bevraging binnen drie units zal uitvoeren. Door de korte stageperiode is het onmogelijk om het onderzoek binnen heel Ordina uit te voeren. Samen met de Business Unit Manager, Mark Vandenwauver, hebben we besloten om de bevraging door volgende units te laten invullen: Busines Platforms Services (BPS), SAP en onze eigen unit Security & Privacy.

Dankzij Mark hebben de Business Unit Managers van BPS en SAP mij de kans gegevens om het concept van mijn onderzoek uit te leggen en op die manier toestemming te krijgen om mijn bevraging binnen hun units uit te voeren. Het leek mij ook belangrijk dat mijn bevraging namens mij door de managers zelf werd doorgestuurd, om zo een gevoel van urgentie te creëren bij de werknemers.

5.3.1 Resultaten

De bevraging stond online voor tien dagen en in totaal hebben, uit de drie verschillende units, 74 werknemers deelgenomen aan mijn bevraging. Voor de SAP en de Business Platform units die dagelijks met persoonsgegevens te maken hebben en deze verwerken, is het van belang dat de werknemers goed op de hoogte zijn van privacy.

De bevraging is opgesteld uit meerkeuzevragen op een drietal open vragen na. De resultaten gaan we verder bespreken aan de hand van "threshold":

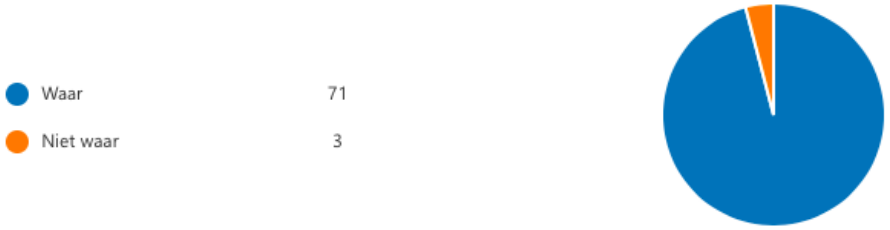
Alle antwoorden boven 95% zijn gewenst en betekent dat de privacy kennis zeer hoog is. Tussen 80% en 95% zijn de antwoorden acceptabel, maar moeten toch in het oog worden gehouden. Tenslotte zijn alle antwoorden onder de 80% ongewenst. Dit betekent dat er dringend nood is aan nieuwe stappen om de privacy awareness van de werknemers te verhogen.

Score	<80%	80% - 95%	>90%

Op onderstaande vragen hebben minimum 95% van de deelnemers juist geantwoord. Op vraag 4 wisten slechts 4% van de respondenten niet dat een e-mailadres een identificeerbare gegeven is. Vraag 6 hebben 97% van de respondenten juist beantwoord, wat te verwachten was van werknemers binnen een IT bedrijf. Vraag 16 werd tot mijn verbazing ook heel goed beantwoord, op 4% na van de deelnemers.

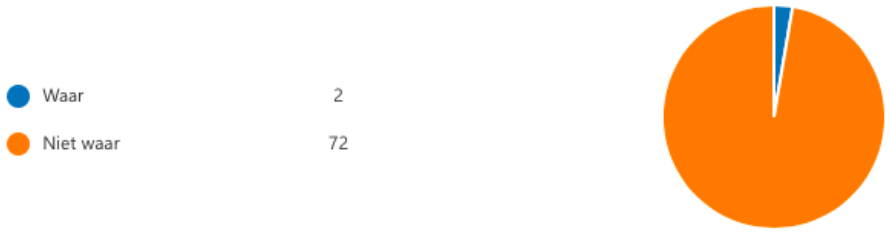
4. Je e-mail adres wordt beschouwd als een persoonsgegeven.

Meer details



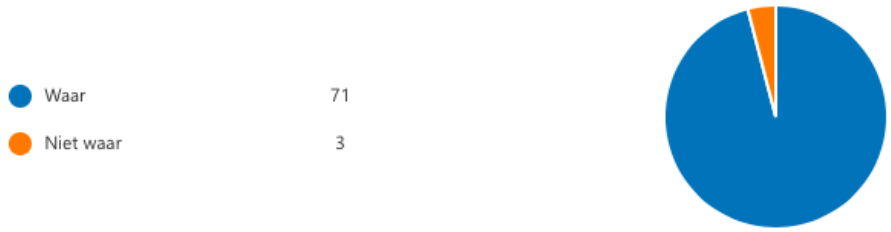
6. We kunnen alleen spreken van een datalek als er gehackt wordt.

Meer details



16. De GDPR geldt zowel voor klanten als werknemers.

Meer details



Aan de hand van onderstaande antwoorden valt er op te merken dat wanneer de vragen diepgaand werden gesteld, er meer fouten werden gemaakt. Hoewel minstens 80% van de deelnemers toch een juiste antwoord hebben gegeven, is het toch verstandig om de awareness regelmatig bij te houden op de werkvloer.

86% van de respondenten hebben het juiste antwoord gegeven op vraag 9, echter wisten de overige 14% van de respondenten niet wat verwerken precies inhoudt.

Op vraag 19 werd in het algemeen correct geantwoord, met 85% juist. Toch konden 14% van de deelnemers een ongeldige toestemming niet herkennen.

Bij vraag 20 merken we dat 84% van de deelnemers het juiste antwoord hebben aangeduid, echter valt er te merken op de volgende vraag dat slechts 27% van de deelnemers dit hebben onthouden van de gevolgde e-learning, 55% van de respondenten hebben erover gehoord van iemand en slechts 5% van de respondenten weten dit toe te passen.

Op vraag 22 en 23 valt weer hetzelfde te zien. 89% van de deelnemers hadden de vraag juist, alleen wisten slechts 27% van de deelnemers dit van de gevolgde e-learning. Liefst 61% van de deelnemers hebben hierover gehoord en de overige 6% van de deelnemers hebben dit al eerder in de praktijk toegepast.

9. Alleen al het opslaan van persoonsgegevens betekent dat de organisatie persoonsgegevens aan het verwerken is.

Meer details

Waar	64
Niet waar	10

19. Jouw onderneming biedt online -filmdiensten aan. Bij het verzamelen van de gegevens die nodig zijn voor die overeenkomst, vraag je ook om aanvullende gegevens zoals de politieke overtuigingen. De betrokkene gelooft dat zijn toestemming voor de verwerking van dit soort gegevens noodzakelijk is om toegang te krijgen tot de films die hij wenst. Is dit een geldige toestemming volgens de GDPR?

Meer details

Ja	4
Nee	63
Weet het niet	7

20. Onderstaande rechten zijn allemaal van toepassing op jou als werknemer: -Recht van inzage en kopie -Recht op beperking -Recht op gegevenswissing -Recht op rectificatie -Recht op vergetelheid

Meer details

Waar	62
Niet waar	12

21. Hoe ben je dit te weten gekomen?

Meer details

De gevolgde e-learning	17
Je hebt dit al eerder in de prak...	5
Je hebt erover gehoord	34
Anders	6

22. Als werknemer kan je geen bezwaar maken op de manier waarop Ordina jouw gegevens gebruikt.

Meer details

Waar	8
Niet waar	66

23. Hoe ben je dit te weten gekomen?

Meer details

De gevolgde e-learning	18
Je hebt dit al eerder in de prak...	4
Je hebt erover gehoord	40
Anders	4

Op volgende vragen hebben de deelnemers het slechtst gescoord. Bij vraag 2 zien we dat 59% het correct hebben beantwoord dat de overige 41% zich heeft laten misleiden door de verschillende keuzes. Bij vraag 7 hebben 77% zich laten misleiden. Dit bevestigt dat de privacy kennis niet genoeg ontwikkeld is en dat 77% niet weet dat ze als eerst moeten kijken naar de risico voor de betrokkene.

Het resultaat op vraag 12 is zorgwekkend. 30% van de respondenten hebben geen kennis van wat een verwerkingsregister precies inhoudt. Nochtans is dit zeker van belang voor de werknemers zelf, om te weten dat hun gegevens op een correcte manier verwerkt worden.

58% heeft een fout antwoord gegeven op vraag 17. Werknemers hebben geen besef dat hun werkgever het recht heeft om toegang te krijgen tot bepaalde informatie, al behoort het tot de bijzondere persoonsgegevens. Het belang van de arbeidsrelatie wordt simpelweg vergeten.

Vraag 18 werd wel juist beantwoord door 77%, echter is dit niet genoeg. 23% hebben zich laten misleiden en dachten niet na over het sociaal secretariaat bijvoorbeeld dat toegang heeft tot bepaalde gegevens voor het uitbetalen van de lonen. Hier werd weer niet gedacht aan de arbeidsrelatie.

Het resultaat op vraag 28 is best interessant. 76% heeft aangegeven dat ze degelijk weten bij wie ze terecht kunnen met vragen omtrent privacy. Echter werd mij duidelijk op basis van de open vraag dat het niet het geval is. Slechts 24% wisten wie de DPO was of hebben privacy@ordina aangegeven.

Het is duidelijk dat werknemers niet helemaal privacy aware zijn. Sommigen hebben een gewenst of acceptabel antwoord kunnen geven op bepaalde vragen, echter werd er slecht gescoord op diepgaande vragen. Door middel van deze vaststelling, rijst de vraag of de gevolgde e-learning wel bij iedereen even lang is blijven hangen.

2. Welke gegeven uit onderstaande lijst is geen persoonsgegeven:

Meer details

Een naam	4
Een gebruikersnaam	13
Een nummerplaat	5
Gegevens over uw organisatie	44
Locatiegegevens	8

7. Mijn laptop van het werk wordt gestolen, moet dit worden gemeld als een datalek?

Meer details

Ja, altijd	57
Ja, soms	15
Nee, nooit	2

12. Is er een verwerkingsregister binnen Ordina?

Meer details

Ja	50
Nee	2
Weet niet wat het is	22

17. Gelet op de arbeidsrelatie, kan jouw werkgever toegang krijgen tot gevoelige persoonsgegevens zoals jouw lidmaatschap bij een vakbond.

Meer details

Waar	31
Niet waar	43

18. Jouw persoonsgegevens mogen gedeeld worden met een derde partij.

Meer details

Waar	0
Waar, onder bepaalde omstan...	57
Niet waar	17

28. Weet je bij wie je terecht kan binnen Ordina indien je vragen hebt omtrent privacy?

Meer details

Ja	56
Nee	18

29. Is er een Data Protection Officer (DPO) aangesteld binnen Ordina? Hoe contacteer je best de DPO?

Meer details

72

Antwoorden

Meest recente antwoorden

"email/phone"

"privacy@ordina.be"

"Is mij ontgaan hoe dit is geregeld binne Ordina, omdat ik slecht 1 ...

5.4 Act

Op basis van deze resultaten, is het duidelijk te zien dat er nog ruimte is voor verbetering binnen Ordina. Op sommige vlakken hebben werknemers iets kunnen onthouden van de verplichte- e-learning, echter is het niet voldoende. Het is van uiterst belang dat bedrijven bewustmaking in het oog houden. Eenmalige bewustwoordingsprogramma's zijn duidelijk weinig effectief, en dit is te merken aan de resultaten. Het is belangrijk om de werkvloer regelmatig te laten stilstaan bij wat ze praktisch kunnen doen rond GDPR en privacy.

Privacy awareness moet natuurlijk gaan van werknemers. Het gaat namelijk gepaard met gedragsverandering. Opdat werknemers zelf interesse tonen, moet het bedrijf ervoor zorgen dat er genoeg geïnvesteerd wordt in goede privacy awareness campagnes.

In deze optiek, begon ik een actieplan met verschillende ideeën uit te werken, die mij interessant en realistisch leken binnen mijn tijdsbestek.

Als eerst dacht ik om een mini-campagne te voeren waarbij ik de resultaten van de bevraging bespreek in een presentatie voor de drie betrokken units. Echter was dit moeilijk in de praktijk waar te maken, aangezien veel werknemers bij hun klanten zijn en niet iedereen tijd kon maken.

Vervolgens begon ik met het ontwerpen van flyers en posters om de serieuze boodschap van de e-learning wat luchtig uit te brengen. Mijn eerste stap was het brainstormen over verschillende slogans en berichten die ik over wou brengen op een duidelijke maar luchtige manier. Verder was het voor mij belangrijk om een design te hebben dat binnen de IT past. Na overleg met mijn collega's, vonden we dat het invoeren van een 'mascotte' de boodschap duidelijker maakt, en meer visualiseert. Hierna ben ik aan de slag gegaan door ons mascotte te ontwerpen via de app 'Bitmoji'.

Tot slot, heb ik een meeting moeten plannen met onze Legal Council en DPO om een goedkeuring te ontvangen, waarna ik al het materiaal mocht afprinten en binnen het gebouw mocht ophangen. En dit juist gelijktijdig met het één-jarig bestaan van de GDPR.

Ten tweede heb ik een actieplan uitgewerkt om een USB-drop test uit te voeren binnen Ordina. Een USB-drop test houdt in dat er verschillende USB-sticks achtergelaten worden met als doel het misleiden van de voorbijgangers om de USB-stick mee te pakken en te gebruiken. Een normaal voorzichtig persoon zou een gevonden USB-stick bij de IT-departement binnenbrengen, omdat het niet te vertrouwen is. Toch is een gevonden USB-stick verleidelijk om te kijken wat er op staan. De bedoeling van de test was het rondstrooien van geprepareerde USB-sticks in het gebouw, waarbij er getest wordt hoe de werknemers het gevaar inzien en de sticks binnenbrengen. Indien de werknemers zich laten misleiden en de USB-stick in de computer steken, verschijnt er een blauw scherm met het woord "GOTCHA". Daarnaast is het ook interessant om te weten wat de reden was voor het aansluiten van de USB-stick. Er zal vervolgens een link verschijnen waarbij ze doorverwezen worden naar een Microsoft Forms file met 1 à 2 feedbackvragen.

Tot slot, heb ik met behulp van mijn stagementor een paar ideeën verder uitgewerkt, die Ordina in de toekomst kan gebruiken in privacy awareness campagnes en trainingen.

Besluit

De wereld waarin wij vandaag de dag leven is zeer afhankelijk van technologie. Waar we toen in 1992 spraken over de bescherming van de persoonlijke levenssfeer, spreken we nu door al de technologische evoluties over de bescherming van persoonsgegevens. Het is ook logisch dat de opvatting die de burgers vroeger gaven aan privacy verschilt van de opvatting die er nu aan wordt gegeven. Er zijn verschillende nieuwe begrippen ontstaan waar de huidige GDPR rekening mee moet houden. Hierbij denken we bijvoorbeeld aan een "DPO" en "DPIA".

Hoewel uniformiteit en harmonisatie het hoofddoel was van de GDPR, werden toch een aantal uitzonderingen onder bepaalde voorwaarden en in bepaalde omstandigheden toegelaten op de reikwijdte van de rechten en plichten uit de verordening. Bijgevolg kunnen de lidstaten bij wet of bij collectieve arbeidsovereenkomst bijkomende regels vaststellen ter bescherming van de verwerkte persoonsgegevens van werknemers in het kader van een arbeidsovereenkomst.

Wat betreft de arbeidsverhouding is het recht op privacy van werknemers duidelijk aan de orde. Echter bestaan er grenzen. De specifieke statuut van het werknemer zijn impliceert een aantal beperkingen aan de privacy van het individu. Hun recht op privacy zal in bepaalde gevallen toch moeten wijken voor andermans rechten of belangen. Het is dus belangrijk om op een juiste manier de verschillende belangen met elkaar te verzoenen.

Om ervoor te zorgen dat privacy een welbesproken thema blijft onder de werknemers, is het noodzakelijk om het onderwerp actueel te houden. Om de bescherming van persoonsgegevens te garanderen als bedrijf, is het belangrijk dat werknemers zich ervan bewust zijn om de gegevens te beschermen, maar ook bewust van hun eigen rechten. Als de awareness er niet is, dan is de kans op risico's erg groot en dit willen we juist vermijden.

Aan de hand van mijn onderzoek, kwamen we tot de conclusie dat privacy awareness niet gemakkelijk te behouden is. Eenmalige bewustwordingscampagnes hebben niet veel effect op de werknemers, waardoor er nood is aan een regelmatige opfrissing. Dit zal de werknemers ook stimuleren om privacy bewust te willen zijn. Er zijn genoeg bewustwordingsmanieren die uitgevoerd kunnen worden en een groot verschil kunnen maken.

Ik heb de kans gekregen om op 1 augustus officieel te beginnen werken bij Ordina. Dit zal mij de mogelijkheid geven om mijn actieplannen verder uit te voeren binnen het bedrijf en om veranderingen te brengen aan de privacy awareness-level bij de werknemers.

Literatuurlijst

Wetgeving

Handvest van de Grondrechten van de Europese Unie.

Verdrag van 25 maart 1957 betreffende de werking van de Europese Unie, *BS* 25 december 1957.

Verdrag van 4 november 1950 tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden, *BS* 19 augustus 1955.

Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, *L 119/1,* 4 mei 2016, 1-88.

Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Nr. L 281/31,* 23 november 1995, 1-10.

Grondwet.

Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 augustus 2018.

Wet 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de veverwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *BS* 2 maart 1999.

Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993.

Wet 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *BS* 21 april 1984.

Considerans 34.

Rechtsleer

- *Boeken*

DE HERT, P. en GUTWIRTH, S., *Anthologie privacy overzicht van artikels wetgeving en rechtsspraak over privacy- en persoonsgegevensbescherming voor België tot 1998,* Brussel, ASP, 2013, 64.

FRIEDEWALD, M. en POHORYLES, R.J., *Privacy and Security in the Digital Age*, Oxon, Routledge, 2016, 212.

OTTO, M., *The Right to Privacy in Employment: A comparative Analysis*, Oxford, Hart Publishing, 2016, 256;

- *Bijdragen in tijdschriften*

BALTHAZAR, T., "Nieuwe kaderwet vormt sluitstuk voor GDPR", *De Juristenkrant* 2018, 1-2.

BALTHAZAR, T., "Privacycommissie wordt Gegevensbeschermingsautoriteit", *DJK* 2018, nr. 362, 2.

CRUYSMANS, E., "Data Protection & Privacy. Le GDPR dans la pratique", RDIDC 2018, nr. 2, 307-310.

DE BACKER, M. en FRANSEN, T., 'Algemene Verordening Gegevensbescherming. Naar een nieuw concept inzake bescherming van persoonsgegevens?", *NJW* 2018, nr. 378, 190-203.

GOOSSENS, G. en VAN CANNEYT, T., "The general data protection regulation: 10 things company lawyers should know", *CDJ* 2016, nr. 1, 1-11.

HENDRICKX, F., "Privacy en arbeidsrecht", *Jura Falc.* 1998-1999, nr. 4, 619-642.

HENROTTE, J.F. en COTON, F., "Everything you always wanted to know about DPO (but were afraid to ask)", *CDJ* 2017, nr. 2, 32-42.

JACOBS, E., "Acht misverstanden over nieuwe Europese privacyverordening, *DJK* 2017, nr. 345, 13.

JANSSENS, K. en NUYTTEN, M., "De Algemene Verordening Persoonsgegevens: van theorie naar praktijk. Le Règlement Général sur la Protection des Données: de la théorie à la pratique", *RDC-TBH* 2018, nr. 5, 401-435.

KEEREMAN, A., "Privacybescherming werknemers in wiskundige formule (interview met Yung Shin Van Der Sype)", *DJK* 2017, nr. 352, 5.

KEEREMAN, A., "Privacy moet voor bedrijven een uitgangspunt zijn", *DJK* 2015, nr. 307, 8-9.

RAETS, S., "Alles wat werkgevers moeten weten over de Algemene Verordening Gegevensbescherming (GDPR)", *ORM* 2016, nr.7, 208-225.

ROYER, S. en YPERMAN, W., "Horen, zien en (moeten) spreken: Grondwettelijk Hof vernietigt actieve meldplicht ocmw's" *DJK* 2019, nr. 386, 1-2.

SAELENS, R. en DE HERT, P., "Raad voor Vreemdelingenbetwisting – Elektronische procesvoering – Privéleven – Bescherming persoonsgegevens – Informatieveiligheid – Bescherming communicatiegeheim", RW 2016-17, nr. 15, 584-588.

SCHOEFS, R., "Witte rook voor nieuwe privacyverordening", *DJK* 2016, nr. 321, 16.

VANDERSTICHELE, G., "Rechtspraak in een datagestuurde informatiemaatschappij", *NJW* 2017, nr. 368, 618-635.

VAN DER SYPE, Y., "De gegevensbeschermingseffectbeoordeling voor de verwerking van werknemersgegevens", *ORM* 2018, nr. 1, 2-11.

VAN DER SYPE, Y.S., "Bescherming van persoonsgegevens in de arbeidscontext anno 2018: enkele uitdagingen voor het rechtmatig verwerken van werknemersgegevens", *Arbeidsrecht Journaal* 2017, 23-29.

VAN DER SYPE, Y., "Een geïntegreerde methode voor de beoordeling van de privacy- en persoonsgegevensbescherming van werknemers", *SK* 2017, nr. 10, 377-398.

VAN GREMBERGHE, T., "GDPR legt procedure vast bij datalekken", *De Juristenkrant* 2017, nr. 358, 7.

VEDDER, A. en VAN DER SYPE, Y., "Privacy, werk en internet of things", *ORM* 2016, nr. 5, 118-127.

Working Group 29, Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens, 18/NL, 26.

Working Group 29, "Opinie 2/2017 on data processing at work", *WP* 249, 2017, 6.

Working Group 29, guidelines on transparency under Regulation 2016/679, 17/EN, 7-8.

X, "Uitzonderingen privacy-wet bij sociale inspectie", *DJK* 2015, nr. 307, 2.

Rechtspraak

HvJ, 13 mei 2014, C-131/12.

Onlinebronnen

CBPL, *Algemene Verordening Gegevensbescherming - Bereid je voor in 13 stappen*, Commissie voor de bescherming van de persoonlijke levenssfeer, 2017, https://gdpr-eu.be/wp-content/uploads/2016/12/STAPPENPLAN-NL-V2.pdf.

Claeys & Engels, *Mag een werkgever nog wel foto's verwerken onder de GDRP?,* Claeys & Engels, 2018, https://www.gdprbelgium.be/nl/nieuws/mag-een-werkgever-nog-wel-foto's-verwerken-onder-de-gdpr.

Dooms Global, *From proposal to law: EU's new Data Protection Regulations*, Dooms Global, 2017, https://drooms.com/en/blog/from-proposal-to-law-eus-new-data-protection-regulations.

ENISA-Conference, https://www.enisa.europa.eu/events/edps-enisa-conference/edps-enisa-conference-towards-accessing-the-risk-in-personal-data-breaches.

Europese Commissie, *Gegevensbescherming in de EU*, Europese Commissie, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_nl.

GBA, *Privacy op de werkvloer: algemeen,* Gegevensbeschermingsautoriteit, https://www.gegevensbeschermingsautoriteit.be/privacy-op-de-werkvloer-algemeen.

GBA, "*Privacycommissie",* https://www.gegevensbeschermingsautoriteit.be/lexicon/privacycommissie, (consultatie 13 maart 2019).

GBA, "Nieuwe privacywetgeving (AVG), https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-0, (consultatie 31 mei 2019).

GDPR-eur, *General Data Protection Regulation*, GDPR-eur, https://gdpr-eu.be/wat-is-gdpr/.

GIJSBRECHTS, K., *De GDPR-wetgeving uitgelegd in vijf vragen,* https://www.smartbiz.be/achtergrond/167961/de-gdpr-wetgeving-uitgelegd-vijf-vragen/.

HUIS, I., "Meten is weten: hoe doe je dat met privacy awareness?", https://www.privacycompany.eu/meten-is-weten-hoe-doe-je-dat-met-privacy-awareness/, (consultatie 29 mei 2019).

Ministerie van Justitie en Veiligheid*, Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*, Ministerie van Justitie en Veiligheid, 2018, file:///C:/Users/ElNa/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/Nieuwe%20Handleiding%20Algemene%20verordening%20gegevensbescherming%20(1).pdf.

RIS-Rijkschroeff Juristen, "De algemene Verordening Gegevensbescherming en awareness", https://www.ris-rijkschroeff.nl/Privacyrecht/De-Algemene-Verordening-Gegevensbescherming-en-awareness, (consultatie 28 mei 2019).

Sustronck, O., *Is er steeds toestemming nodig voor direct marketing?,* Wolters Kluwer, https://gdpr.wolterskluwer.be/nl/nieuws/is-er-steeds-toestemming-nodig-voor-direct-marketing/.

X, "Achtergrond van de AVG", https://avg-compleet.nl/blog/achtergrond-van-de-avg/,(consultatie 29 mei 2019).

X, PDCA-cycle (figuur 1). Geraadpleegd van https://www.patagonia-bv.com/kwaliteitsmanagementsystemen/plan-do-check-act-pdca/.

Overzicht van de bijlagen

- Bijlage 1: Model privacyverklaring tussen werkgever en werknemer.
- Bijlage 2: Template verwerkingsregister.
- Bijlage 3: Bevraging privacy awareness.

Bijlage 1: Model privacyverklaring tussen werkgever en werknemer[101]

Privacyverklaring tussen werkgever en werknemer

In deze privacyverklaring wordt verstaan onder (i) 'werkgever': [naam onderneming], [adres], [ondernemingsnummer] en (ii) 'werknemer': hij of zij die zich verbindt in dienst van de andere partij, de werkgever, tegen loon arbeid te verrichten.

Persoonsgegevens

1. Bescherming van persoonsgegevens

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

De werkgever hecht het nodige belang aan het respecteren en de bescherming van de privacy en de vertrouwelijkheid van de persoonsgegevens van de werknemer. Onderhavige privacyverklaring heeft tot doel de werknemer te informeren over de modaliteiten in verband met het gebruik van persoonsgegevens en over de ingestelde beschermingsregels om de vertrouwelijkheid van deze persoonsgegevens te vrijwaren.

De werkgever verbindt zich ertoe om persoonsgegevens discreet te gebruiken en het vertrouwelijke en private karakter ervan te beschermen. Dit alles in overeenstemming met de Algemene Verordening Gegevens-bescherming (GDPR), de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (zoals gewijzigd) (hierna 'de Wet van 8 december 1992') en de andere relevante vigerende wettelijke voorschriften. De werkgever heeft naar best vermogen juridische en technische voorzorgen genomen om ongeoorloofde toegang tot en gebruik van de persoonsgegevens te vermijden. Waar het onmogelijk is om beveiliging volledig te kunnen garanderen, zal de werkgever voorzien in passende technische en organisatorische maatregelen om de persoonsgegevens te beschermen.

2. Welke persoonsgegevens worden verzameld, waarom en voor welke doeleinden?

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of

[101] Eubelius, template privacyverlaring.

vernietigen van gegevens.

"Vertrouwelijke verwerking" betekent dat de werkgever de persoonsgegevens op vertrouwelijke wijze verwerken overeenkomstig de in België geldende wettelijke voorschriften, met name de Algemene Verordening Gegevensbescherming (GDPR) en de Wet van 8 december 1992.

De werkgever kan de volgende **persoonsgegevens** van de werknemer *(bv. naam, voornaam, rijksregisternummer, telefoonnummer, adres, e-mailadres, rekeningnummer, afbeelding, gezinssamenstelling, opleiding, functie, etc.)* verwerken op basis van volgende **rechtsgronden** *(toestemming van de werknemer, noodzakelijkheid voor de uitvoering van de arbeidsovereenkomst, wettelijke verplichting, bescherming van vitale belangen, taak van algemeen belang of gerechtvaardigd belang)* voor volgende **doeleinden** *(bv. om te voldoen aan wettelijke verplichtingen (personeelsbeheer, etc.), om de arbeidsovereenkomst te kunnen uitvoeren, om de werknemer te voorzien van informatieve nieuwsberichten m.b.t. de onderneming, om de kwaliteit van diensten of informatie te verbeteren, om de veiligheid en toegang tot de onderneming te waarborgen, etc.)*:

Persoonsgegevens	Rechtsgrond	Doeleinde
Naam, voornaam, adres, rijksregisternummer, gezinssamenstelling, opleiding, functie	Wettelijke verplichting	Beheer van personeelsdossiers
E-mailadres	Toestemming van de werknemer	Voorzien van informatieve nieuwsberichten m.b.t. de onderneming

[informatie in bovenstaande tabel schrappen/aanvullen]

Door persoonsgegevens te verstrekken, verleent de werknemer de uitdrukkelijke toestemming om die gegevens te verwerken voor de bovengenoemde doeleinden. De werknemer heeft het recht om de gegeven toestemming terug in te trekken, voor zover de verwerking louter gebaseerd is op de toestemming van de werknemer.

Tevens stemt de werknemer er uitdrukkelijk mee in dat de persoonsgegevens in het kader van de verwerking en in overeenstemming met de wettelijke bepalingen kunnen worden meegedeeld aan volgende ontvangers binnen de Europese Economische Ruimte:

- het sociaal secretariaat van de werkgever: [naam + contactgegevens]
- dochterondernemingen van de werkgever: [naam + contactgegevens]
- commerciële partners van de werkgever: [naam + contactgegevens]

[ontvangers schrappen/aanvullen]

De werkgever garandeert dat deze ontvangers de nodige technische en organisatorische maatregelen zullen nemen ter bescherming van de persoonsgegevens. Indien de werknemer niet wenst dat de persoonsgegevens worden overgemaakt aan derden en de verwerking louter is gebaseerd op de toestemming van de werknemer, kan de werknemer zich hiertegen verzetten hetzij op het ogenblik dat de werknemer de persoonsgegevens verstrekt hetzij op elk ogenblik middels zijn recht op bezwaar of zijn recht op gegevenswissing.

De bewaartermijn van de persoonsgegevens bij de werkgever bedraagt [termijn]. Bij verloop van deze termijn worden de persoonsgegevens automatisch verwijderd uit het systeem. De persoonsgegevens verwerkt voor personeelsbeheer zullen worden bewaard gedurende de termijn die noodzakelijk is om aan de wettelijke vereisten te voldoen (onder andere op het gebied van boekhouding en sociale wetgeving). Indien de werkgever de persoonsgegevens na verloop van de bewaartermijn nog verder wenst te gebruiken, zal de werkgever hiervoor opnieuw toestemming vragen.

3. De rechten van de werknemer

Overeenkomstig de geldende regelgeving en onder de geldende voorwaarden beschikt de werknemer op eenvoudig verzoek over een wettelijk recht op gratis toegang tot zijn persoonsgegevens teneinde deze aan te vullen, te verbeteren, te wijzigen, te verwijderen of over te dragen. De werknemer beschikt eveneens over het recht om zich op eenvoudig verzoek kosteloos te verzetten tegen de verwerking van zijn persoonsgegevens voor doeleinden zoals direct marketing.

Meer specifiek heeft de werknemer overeenkomstig de geldende regelgeving en onder de geldende voorwaarden de volgende rechten:

Recht op inzage: de werknemer heeft steeds de mogelijkheid om zijn persoonsgegevens (incl. verwerkingsdoeleinden, categorieën van persoonsgegevens, verwachte opslagtermijn) op te vragen ter inzage.

Recht op rectificatie: de werknemer heeft steeds de mogelijkheid om zijn persoonsgegevens te laten verbeteren of aan te vullen.

Recht op gegevenswissing: de werknemer heeft onder voorwaarden de mogelijkheid om op simpel kosteloos verzoek de verwijdering van zijn persoonsgegevens te vragen.

Recht op beperking van de verwerking: de werknemer heeft onder voorwaarden de mogelijkheid om een beperking van de verwerking van zijn persoonsgegevens naar de toekomst toe te vragen.

Recht op bezwaar: de werknemer heeft onder voorwaarden de mogelijkheid om een bezwaar in te dienen tegen de verwerking van zijn persoonsgegevens voor onder meer direct marketing doeleinden.

Recht op overdraagbaarheid: de werknemer heeft de mogelijkheid om zijn persoonsgegevens in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen en over te dragen aan derden.

Indien de werknemer één van deze rechten wenst uit te oefenen, kan de werknemer de werkgever schriftelijk contacteren via het e-mailadres [e-mailadres] hetzij via de bovenstaande contactgegevens. De werkgever neemt binnen [termijn] na het verzoek contact op met de werknemer.

Contact

Nog vragen?

De werkgever is de verantwoordelijke voor de verwerking van de persoonsgegevens. Indien de werknemer na het lezen van deze privacyverklaring nog vragen of opmerkingen omtrent de bescherming van zijn persoonsgegevens heeft, kan de werknemer de werkgever contacteren via het e-mailadres [e-mailadres] hetzij via de bovenstaande contactgegevens. De werkgever neemt binnen [termijn] na het verzoek contact op met de werknemer.

[De werknemer kan eveneens contact opnemen met de functionaris voor gegevensbescherming (DPO) die instaat voor de behartiging van de privacybelangen. De werknemer kan de functionaris voor gegevensbescherming (DPO) rechtstreeks bereiken via volgende gegevens: [naam] [voornaam] [e-mailadres] [telefoonnummer].]

Voor bijkomende informatie betreffende de bescherming van de persoonsgegevens kan de werknemer zich richten tot de Gegevensbeschermingsautoriteit te 1000 Brussel, Drukpersstraat 35, tel: 02/274.48.00, e-mail: contact@apd-bga.be, www.gegevensbeschermingsautoriteit.be.

* * *

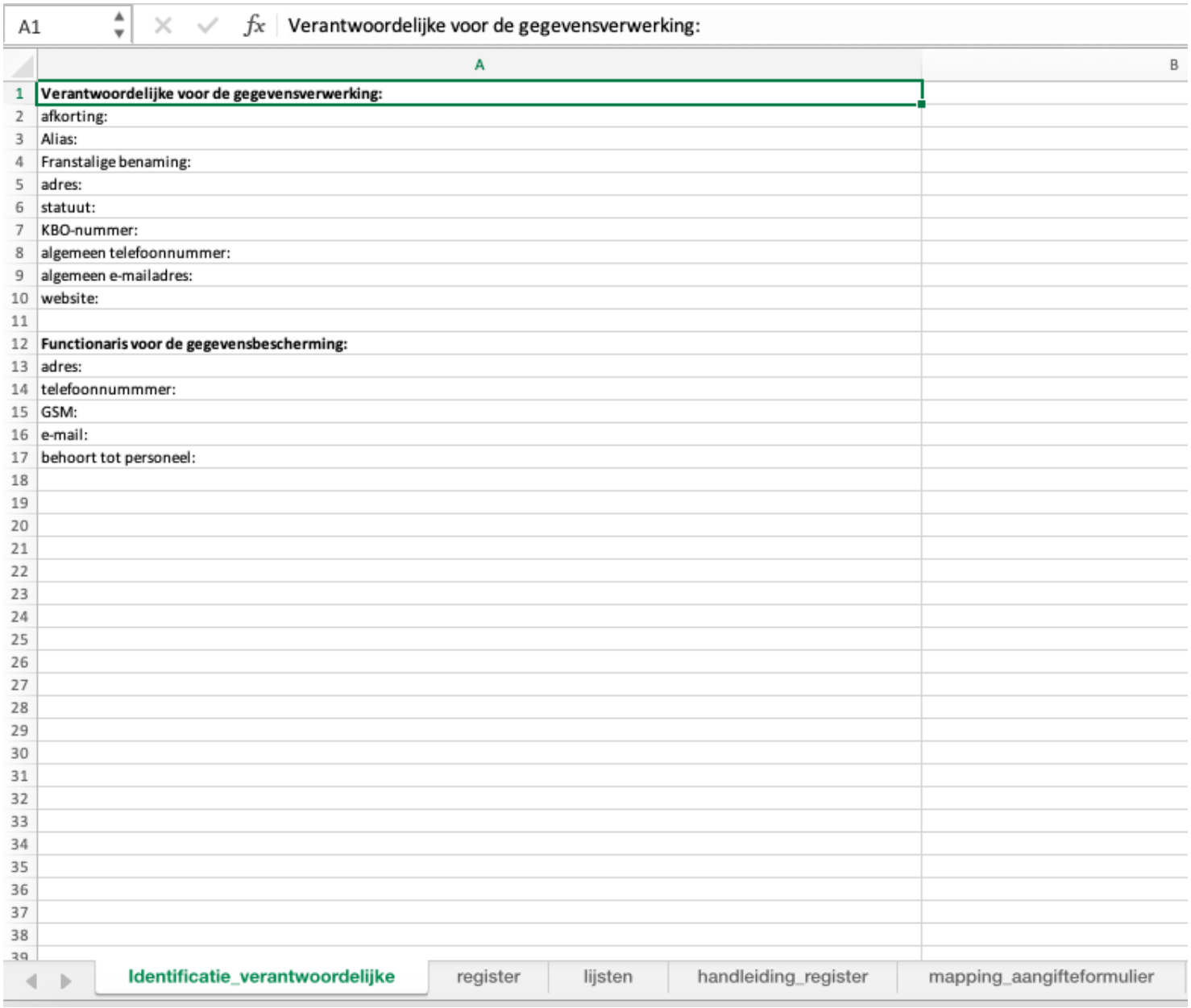
De werknemer verklaart hierbij de privacyverklaring te hebben gelezen en te hebben goedgekeurd. Hierna “gelezen en goedgekeurd”, de datum en handtekening van de werknemer:

_____

Naam werknemer:

Datum:

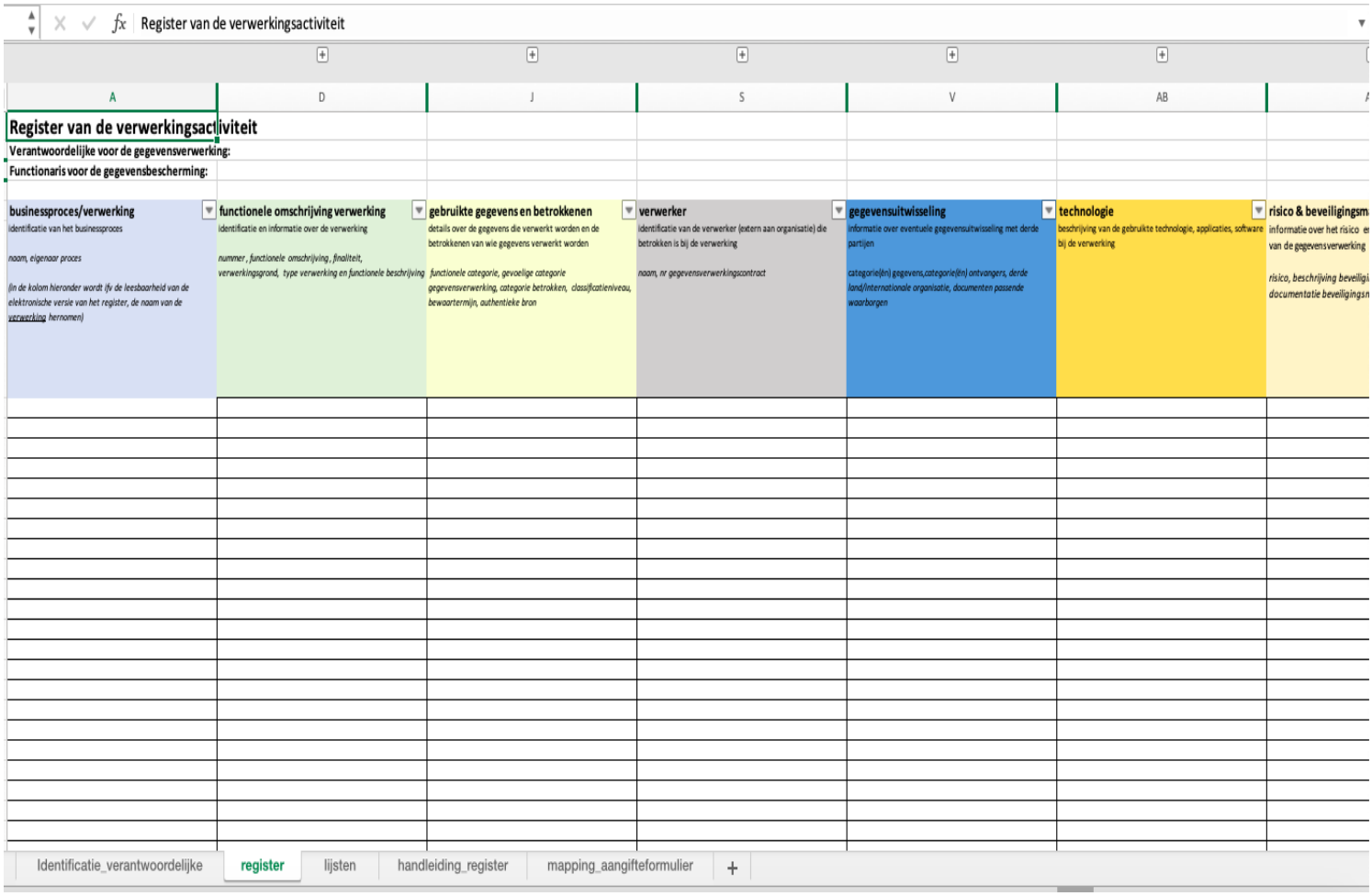
Bijlage 2: Template verwerkingsregister[102]

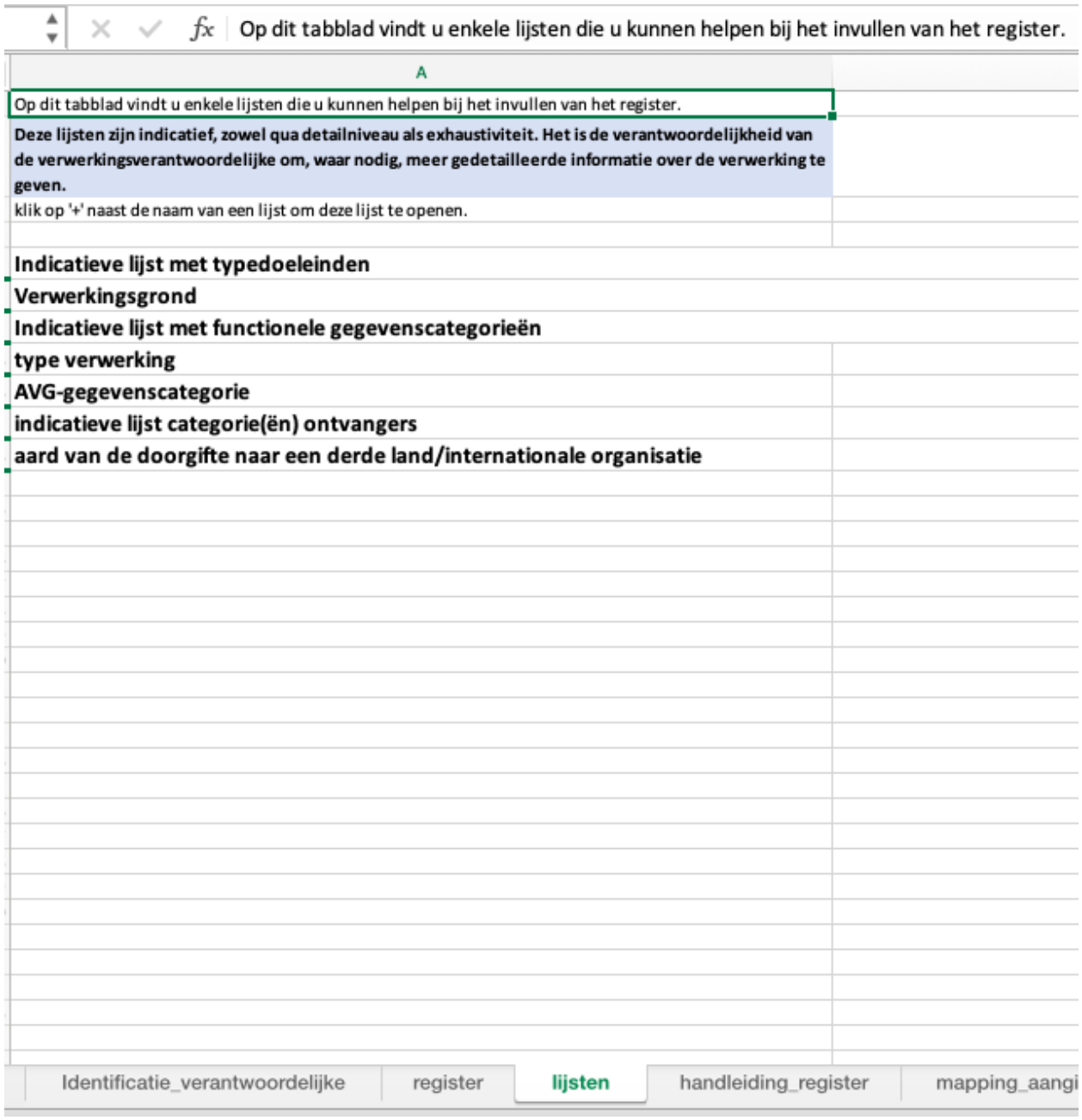


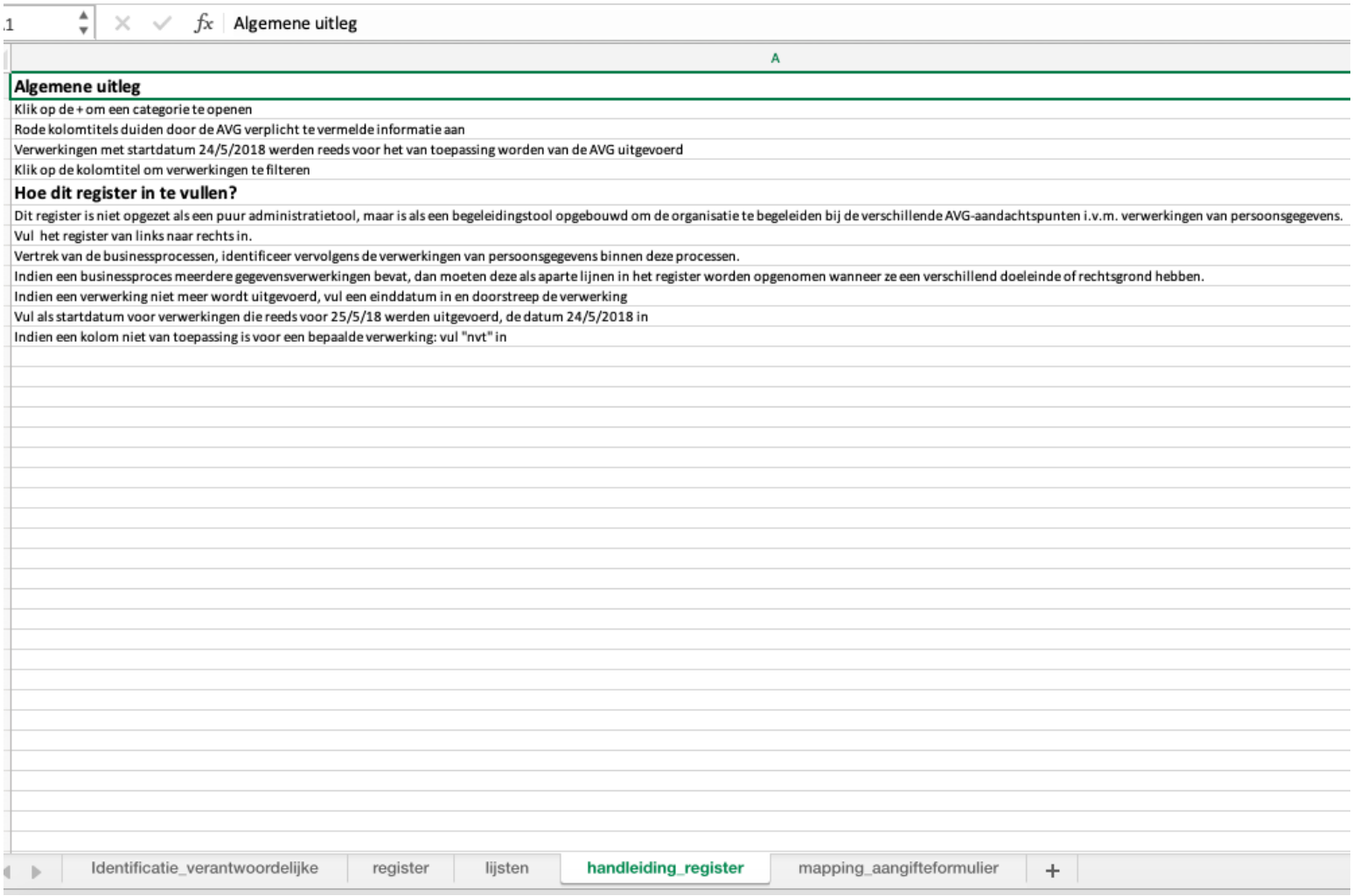
A1 | Verantwoordelijke voor de gegevensverwerking:

	A	B
1	**Verantwoordelijke voor de gegevensverwerking:**	
2	afkorting:	
3	Alias:	
4	Franstalige benaming:	
5	adres:	
6	statuut:	
7	KBO-nummer:	
8	algemeen telefoonnummer:	
9	algemeen e-mailadres:	
10	website:	
11		
12	**Functionaris voor de gegevensbescherming:**	
13	adres:	
14	telefoonnummmer:	
15	GSM:	
16	e-mail:	
17	behoort tot personeel:	
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		
36		
37		
38		
39		

[102] Gegevensbeschermingsautoriteit, template verwerkingsregister.


Register van de verwerkingsactiviteit
A
D
J
S
V
AB
Register van de verwerkingsactiviteit
Verantwoordelijke voor de gegevensverwerking:
Functionaris voor de gegevensbescherming:
businessproces/verwerking
identificatie van het businessproces
naam, eigenaar proces
(in de kolom hieronder wordt (fv de leesbaarheid van de elektronische versie van het register, de naam van de verwerking hernomen)
functionele omschrijving verwerking
identificatie en informatie over de verwerking
nummer , functionele omschrijving , finaliteit, verwerkingsgrond, type verwerking en functionele beschrijving
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
verwerker
identificatie van de verwerker (extern aan organisatie) die betrokken is bij de verwerking
naam, nr gegevensverwerkingscontract
gegevensuitwisseling
informatie over eventuele gegevensuitwisseling met derde partijen
categorie(ën) gegevens,categorie(ën) ontvangers, derde land/internationale organisatie, documenten passende waarborgen
technologie
beschrijving van de gebruikte technologie, applicaties, software bij de verwerking
risico & beveiligingsm
informatie over het risico e
van de gegevensverwerking
risico, beschrijving beveiligi
documentatie beveiligingsm
Identificatie_verantwoordelijke
register
lijsten
handleiding_register
mapping_aangifteformulier
+


Op dit tabblad vindt u enkele lijsten die u kunnen helpen bij het invullen van het register.
A
Op dit tabblad vindt u enkele lijsten die u kunnen helpen bij het invullen van het register.
Deze lijsten zijn indicatief, zowel qua detailniveau als exhaustiviteit. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om, waar nodig, meer gedetailleerde informatie over de verwerking te geven.
klik op '+' naast de naam van een lijst om deze lijst te openen.
Indicatieve lijst met typedoeleinden
Verwerkingsgrond
Indicatieve lijst met functionele gegevenscategorieën
type verwerking
AVG-gegevenscategorie
indicatieve lijst categorie(ën) ontvangers
aard van de doorgifte naar een derde land/internationale organisatie
Identificatie_verantwoordelijke
register
lijsten
handleiding_register
mapping_aangi


A1
Algemene uitleg
A
Algemene uitleg
Klik op de + om een categorie te openen
Rode kolomtitels duiden door de AVG verplicht te vermelde informatie aan
Verwerkingen met startdatum 24/5/2018 werden reeds voor het van toepassing worden van de AVG uitgevoerd
Klik op de kolomtitel om verwerkingen te filteren
Hoe dit register in te vullen?
Dit register is niet opgezet als een puur administratietool, maar is als een begeleidingstool opgebouwd om de organisatie te begeleiden bij de verschillende AVG-aandachtspunten i.v.m. verwerkingen van persoonsgegevens.
Vul het register van links naar rechts in.
Vertrek van de businessprocessen, identificeer vervolgens de verwerkingen van persoonsgegevens binnen deze processen.
Indien een businessproces meerdere gegevensverwerkingen bevat, dan moeten deze als aparte lijnen in het register worden opgenomen wanneer ze een verschillend doeleinde of rechtsgrond hebben.
Indien een verwerking niet meer wordt uitgevoerd, vul een einddatum in en doorstreep de verwerking
Vul als startdatum voor verwerkingen die reeds voor 25/5/18 werden uitgevoerd, de datum 24/5/2018 in
Indien een kolom niet van toepassing is voor een bepaalde verwerking: vul "nvt" in
Identificatie_verantwoordelijke
register
lijsten
handleiding_register
mapping_aangifteformulier

A1 | Kolomtitel template

Kolomtitel template	Rubriek in aangifteformulier
verwerking	1. benaming van de verwerking
doel verwerking	2. doel of geheel van samenhangende doeleinden waarvoor gegevens worden verwerkt
verwerkingsgrond	4. wettelijke of reglementaire basis(sen)
functionele gegevenscategorie	3. categorieën van gegevens die verwerkt worden
categorie betrokkenen	informatie niet opgenomen in aangiften
bewaartermijn	10. voorziene bewaartermijn
categorie gegevens	5. Categorieën ontvangers en categorieën gegevens die kunnen worden verstrekt
Categorie(ën) ontvangers	5. Categorieën ontvangers en categorieën gegevens die kunnen worden verstrekt
derde land/internationale organisatie	12. gegevens die naar het buitenland worden gezonden
documenten passende waarborgen	6. welke maatregelen zijn er genomen om de mededeling van gegevens aan derden te beveiligen? (let op enkel als er sprake is van de situatie art.49.2 AVG)
beschrijving beveiligingsmaatregelen	11. algemene beschrijving van de veiligheidsmaatregelen 6. welke maatregelen zijn er genomen om de mededeling van gegevens aan derden te beveiligen? (indien doorgifte van gegevens)
informeren betrokkenen	7. hoe worden betrokkenen in kennis gesteld van de registratie van hun gegevens?
procedure uitoefenen rechten	9.Bijzondere maatregelen voor de uitoefening van de rechten

Identificatie_verantwoordelijke | register | lijsten | handleiding_register | mapping_aangifteformulier | +

Bijlage 3: Bevraging privacy awareness

Forms

Voorbeeld | Thema | Delen | ...

Opgeslagen

Vragen | Antwoorden 74

Privacy awareness

Beste collega's

Fijn dat jullie deelnemen aan deze vragenlijst.

Sinds 25 mei 2018 is er heel wat veranderd met de opkomst van de GDPR-wetgeving. Bedrijven werden verplicht om zich te houden aan een heleboel regels. In de praktijk kan dit echter nog wat moeilijk zijn.

Met deze vragenlijst komen zowel jullie als ik te weten hoe de privacy awareness binnen Ordina is. Eveneens kan de deelname interessant zijn om te weten te komen welke persoonsgegevens over jullie als werknemers worden verzameld en verwerkt.

Ik hoop dat er oprecht wordt geantwoord op de vragen. Daardoor zijn de resultaten betrouwbaar en natuurlijk levert u een wezenlijke bijdrage aan mijn thesis.

Ik dank jullie alvast!

Nassima El Kindi
Stagiaire Security & Privacy

1

Heb je al eerder gehoord van de GDPR? *

- Ja
- Nee

2

Welke gegeven uit onderstaande lijst is geen persoonsgegeven: *

- Een naam
- Een gebruikersnaam
- Een nummerplaat
- Gegevens over uw organisatie
- Locatiegegevens

Persoonsgegevens als iemands godsdienst worden door de GDPR beschouwd als bijzondere persoonsgegevens. *

- Waar
- Niet waar

4

Je e-mail adres wordt beschouwd als een persoonsgegeven. *

- Waar
- Niet waar

5

De GDPR zorgt voor sterkere privacyrechten. *

- Waar
- Niet waar

6

We kunnen alleen spreken van een datalek als er gehackt wordt. *

- Waar
- Niet waar

7

Mijn laptop van het werk wordt gestolen, moet dit worden gemeld als een datalek? *

- Ja, altijd
- Ja, soms
- Nee, nooit

8

Wanneer een werknemer verzoekt om al zijn persoonsgegevens te verwijderen, moet hier altijd aan worden voldaan. *

- Waar
- Niet waar

9

Alleen al het opslaan van persoonsgegevens betekent dat de organisatie persoonsgegevens aan het verwerken is. *

- Waar
- Niet waar

10

Jouw werkgever is een verwerkingsverantwoordelijke van jouw persoonsgegevens. *

- Waar
- Niet waar

11

Het sociaal secretariaat kan een verwerker zijn. *

- Waar
- Niet waar

12

Is er een verwerkingsregister binnen Ordina? *

- Ja
- Nee
- Weet niet wat het is

13

Ordina heeft een Richtlijn Datalek persoonsgegevens opgesteld om te kunnen voldoen aan de meldplicht voor datalekken. *

- Ja
- Nee
- Weet het niet

Heb je al een privacy awareness training gehad? Intern bij Ordina of extern bij de klant? *

- Ja
- Nee
- Weet het niet

15

Hoe heb je de training ervaren? *

☆ ☆ ☆ ☆ ☆

16

De GDPR geldt zowel voor klanten als werknemers. *

- Waar
- Niet waar

17

Gelet op de arbeidsrelatie, kan jouw werkgever toegang krijgen tot gevoelige persoonsgegevens zoals jouw lidmaatschap bij een vakbond. *

- Waar
- Niet waar

18

Jouw persoonsgegevens mogen gedeeld worden met een derde partij. *

- Waar
- Waar, onder bepaalde omstandigheden
- Niet waar

19

Jouw onderneming biedt online -filmdiensten aan. Bij het verzamelen van de gegevens die nodig zijn voor die overeenkomst, vraag je ook om aanvullende gegevens zoals de politieke overtuigingen. De betrokkene gelooft dat zijn toestemming voor de verwerking van dit soort gegevens noodzakelijk is om toegang te krijgen tot de films die hij wenst.

Is dit een geldige toestemming volgens de GDPR? *

- Ja
- Nee
- Weet het niet

20

Onderstaande rechten zijn allemaal van toepassing op jou als werknemer:

-Recht van inzage en kopie
-Recht op beperking
-Recht op gegevenswissing
-Recht op rectificatie
-Recht op vergetelheid *

- Waar
- Niet waar

21

Hoe ben je dit te weten gekomen? *

- De gevolgde e-learning
- Je hebt dit al eerder in de praktijk gezet
- Je hebt erover gehoord
- Anders

22

Als werknemer kan je geen bezwaar maken op de manier waarop Ordina jouw gegevens gebruikt. *

- Waar
- Niet waar

23

Hoe ben je dit te weten gekomen? *

- De gevolgde e-learning
- Je hebt dit al eerder in de praktijk gezet
- Je hebt erover gehoord
- Anders

24

Als je bezwaar maakt tegen de verwerking van je gegevens, moet hier altijd aan worden voldaan. *

- Waar
- Niet waar

25

Hoe ben je dit te weten gekomen? *

- De gevolgde e-learning
- Je hebt dit al eerder in de praktijk gezet
- Je hebt erover gehoord
- Anders

26

Als werknemer heb je geen recht om een klacht in te dienen bij een toezichthoudende autoriteit. *

- Waar
- Niet waar

27

Hoe ben je dit te weten gekomen? *

- De gevolgde e-learning
- Je hebt dit al eerder in de praktijk gezet
- Je hebt erover gehoord
- Anders

28

Weet je bij wie je terecht kan binnen Ordina indien je vragen hebt omtrent privacy? *

- Ja
- Nee

29

Is er een Data Protection Officer (DPO) aangesteld binnen Ordina? Hoe contacteer je best de DPO? *

Voer uw antwoord in

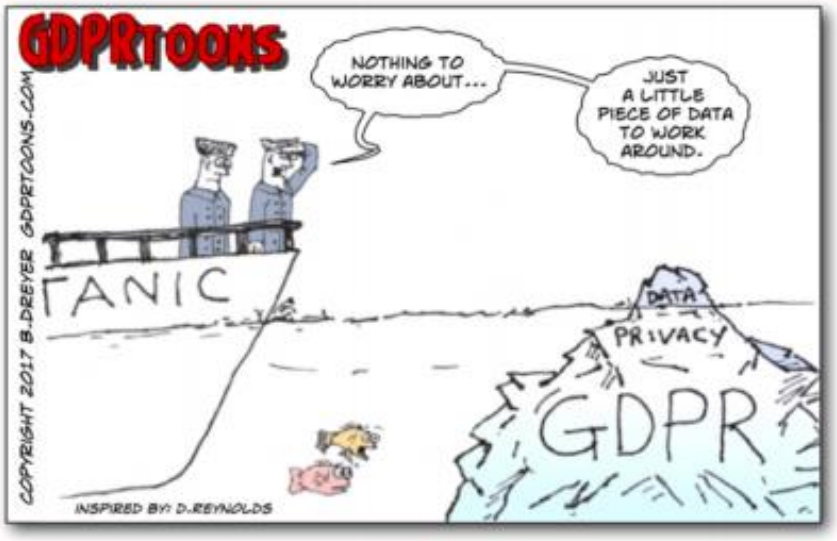
30

Op een schaal van 1 tot 10, hoe beoordeel je jouw huidige privacy awareness niveau? *

1 2 3 4 5 6 7 8 9 10

31

Op een schaal van 1 tot 10, hoe beoordeel je de GDPR-compliance niveau binnen Ordina? *



1 2 3 4 5 6 7 8 9 10

○ ○ ○ ○ ○ ○ ○ ○ ○ ○

+ Nieuwe toevoegen