Revue de l'Union professionnelle des Délégués à la protection des données de Belgique (dpo pro)

Tijdschrift van de Beroepsvereniging van de Data protection Officers in België (dpo pro)

DPO pro mag

Trimestriel/Driemaandelijks * 2025/3

www.dpopromag.be

Édito

Dpo pro en pleine évolution !

Le conseil d'administration de dpo pro ne chôme pas ; il y a de nombreux chantiers sur la table et vous pourrez bien entendu y participer.

Lors de la dernière réunion stratégique du conseil d'administration, un certain nombre de décisions ont été prises et nous souhaitons vous les partager.

Tout d'abord, nous avons redéfini notre mission et nos valeurs.

La mission de dpo pro est désormais la suivante : « dpopro est l'association professionnelle des DPO dédiée à l'aide et l'assistance des DPO et des privacy professionnals ».

Les valeurs que nous affirmons sont :

- la défense des intérêts du secteur ;
- l'expertise ;
- le professionnalisme ;
- la coopération ;
- le partage.

Afin de nous rencontrer plus souvent, nous allons organiser une fois par trimestre une réunion en présentiel sans oublier, bien sûr, les webinaires qui continuent, tout comme le dpo day qui aura lieu à la FEB le 26 mai 2026 à partir de 14 h (Save the date !).

Un nouveau site internet est en développement afin d'améliorer notre interaction avec les membres et le secteur.

Nous préparons une enquête auprès du secteur en collaboration avec l'APD afin de déterminer les sujets qui préoccupent les professionnels.

Après la première réunion d'un groupe de travail consacré au secteur de la santé, un autre groupe de travail consacré au secteur public est en préparation. Des partenariats sont en discussions avec d'autres organisations.

Lors de la prochaine assemblée générale ordinaire, quatre postes d'administrateurs seront à pourvoir, trois du rôle néerlandophone et un du rôle francophone. Nous serions ravis d'accueillir de nouveaux administrateurs car certains administrateurs actuels souhaitent passer la main après de longues années au sein du conseil d'administration. Nous les remercierons lors de l'assemblée générale. N'hésitez donc pas à poser votre candidature et à nous contacter si vous voulez plus d'informations sur le rôle des administrateurs. Il y a, comme vous le voyez, de nombreuses tâches à accomplir et nous avons besoin d'administrateurs qui s'engagent à prendre en charge un des nouveaux projets, voire à en proposer d'autres.

Dpo pro reste donc aux côtés des DPO et des professionnels et innove pour être encore plus à vos côtés.

Jacques Folon
Vice-président de dpo pro

dpo pro

Anthemis

Dpo pro in volle beweging!

De raad van bestuur van dpo pro zit niet stil, er liggen tal van projecten op stapel en u kunt daar natuurlijk aan deelnemen.

Tijdens de laatste strategische vergadering van de raad van bestuur zijn een aantal beslissingen genomen die we graag met u willen delen.

Allereerst hebben we onze missie en onze waarden opnieuw vastgelegd.

De missie van dpo pro is nu als volgt: "dpo pro is de beroepsvereniging van DPO's die zich inzet voor de ondersteuning en bijstand van DPO's en privacyprofessionals".

De waarden die wij uitdragen zijn:

- het behartigen van de belangen van de sector;
- expertise;
- professionaliteit;
- samenwerking;
- uitwisseling.

Om elkaar vaker te kunnen ontmoeten, zullen we eens per kwartaal een fysieke bijeenkomst organiseren, naast de webinars die gewoon doorgaan, zoals de dpo day die op 26 mei 2026 vanaf 14.00 uur plaatsvindt in de FEB (save the date!).

Op dit ogenblik wordt er een nieuwe website ontwikkeld om onze interactie met de leden en de sector te verbeteren.

We bereiden een enquête voor in samenwerking met de Gegevensbeschermingsautoriteit om te bepalen welke onderwerpen de professionals aanbelangen.

Na de eerste vergadering van een werkgroep gewijd aan de gezondheidssector, is een andere werkgroep gewijd aan de publieke sector in voorbereiding. Partnerschappen met andere organisaties worden besproken.

Tijdens de volgende gewone algemene vergadering zullen er vier bestuursfuncties vacant zijn: drie voor Nederlandstaligen en één voor Franstaligen. We zouden graag nieuwe bestuursleden verwelkomen, aangezien sommige huidige bestuursleden na vele jaren in het bestuur het stokje willen doorgeven. We zullen hen tijdens de algemene vergadering bedanken. Aarzel dus niet om u kandidaat te stellen en contact met ons op te nemen als u meer informatie wilt over de rol van bestuurder. Zoals u ziet, zijn er tal van taken te vervullen en hebben we bestuurders nodig die zich willen inzetten voor een van de nieuwe projecten of zelfs nieuwe projecten willen voorstellen.

Zoals u ziet, blijft dpo pro aan de zijde van DPO's en professionals staan en innoveert het om u nog beter van dienst te kunnen zijn.

Jacques Folon
Vicevoorzitter van dpo pro

News

Internationaal/International

- ***Verenigde Staten/États-Unis***

27/05/25

Na langdurig overleg met zijn leidende gegevensbeschermingsautoriteit (de Ierse DPC) is Meta van plan om voortaan openbare inhoud die op Facebook en Instagram wordt gepubliceerd (berichten en reacties, met uitzondering van privéberichten) te gebruiken om zijn generatieve kunstmatige-intelligentiemodellen te trainen. Deze verwerking zal plaatsvinden zonder de uitdrukkelijke toestemming van de gebruikers te vragen, wat ernstige juridische vragen oproept met betrekking tot de AVG. Meta beroept zich op zijn legitieme belangen om deze verwerking te rechtvaardigen, op basis van een advies van het Europees Comité voor gegevensbescherming (EDPB) van eind 2024. We moeten echter niet vergeten dat in het advies van het EDPB werd vermeld dat deze belangen alleen geldig zijn als het gebruik 'absoluut noodzakelijk' is, een voorwaarde die door verschillende autoriteiten als vaag wordt beschouwd. Critici, met name in Duitsland (Noordrijn-Westfalen), veroordelen deze strategie als duidelijk in strijd met de AVG. Het standpunt van Meta, in combinatie met een mogelijke verwerking van gevoelige gegevens, zou tot nieuwe sancties kunnen leiden, maar het Amerikaanse bedrijf lijkt bereid dit risico te nemen om een concurrentievoordeel op het gebied van AI te behouden, aangezien het gebruik van hoogwaardige persoonsgegevens cruciaal is voor de ontwikkeling van krachtige AI-tools. In dit verband overweegt de Oostenrijkse vereniging Noyb (die ook de mogelijkheid overweegt om later een collectieve rechtszaak aan te spannen om schadevergoeding te eisen) heeft op 14 mei 2025 een aanmaningsbrief naar Meta gestuurd om deze verwerkingen te voorkomen. Tot slot zij opgemerkt dat een Duitse rechtbank (het hof van beroep van Keulen), die in spoedeisende zaken is aangezocht, de aanpak van Meta voorlopig heeft bekrachtigd.

Après en avoir longuement discuté avec son autorité de protection des données chef de file (la DPC irlandaise), Meta prévoit de dorénavant utiliser les contenus publics publiés sur Facebook et Instagram (messages et commentaires, hors messages privés) pour entraîner ses modèles d'intelligence artificielle générative. Ce traitement s'effectuera sans demander le consentement explicite des utilisateurs, ce qui soulève de sérieuses questions juridiques au regard du RGPD. Meta invoque ses intérêts légitimes pour justifier ce traitement, s'appuyant sur un avis du Comité européen de la protection des données (EDPB) de fin 2024. Toutefois, rappelons que l'avis de l'EDPB précisait que ces intérêts ne sont valables que si l'usage est «absolument nécessaire», condition jugée floue par plusieurs autorités. Des critiques, notamment en Allemagne (Rhénanie du Nord-Westphalie), dénoncent

cette stratégie comme clairement contraire au RGPD. La position de Meta, combinée à un possible traitement de données sensibles, pourrait entraîner de nouvelles sanctions, mais l'entreprise américaine semble prête à en assumer le risque pour conserver un avantage concurrentiel dans le domaine de l'IA, l'utilisation de données personnelles de qualité étant cruciale pour la mise au point d'outils d'IA performants. À ce sujet, l'association autrichienne Noyb (qui envisage également la possibilité de lancer une action collective ultérieurement afin de réclamer des dommages et intérêts) a envoyé le 14 mai 2025 une lettre de mise en demeure à Meta dans le but d'empêcher ces traitements. Enfin, notez qu'un tribunal allemand (la Cour d'appel de Cologne), saisi en urgence, a, provisoirement, validé l'approche de Meta.

Links : www.dataprotection.ie/en/news-media/latest-news/dpc-statement-meta-ai
www.facebook.com/privacy/genai
https://noyb.eu/en/noyb-sends-meta-cease-and-desist-letter-over-ai-training-european-class-action-potential-next-step
https://nrwe.justiz.nrw.de/olgs/koeln/j2025/15_UKl_2_25_Urteil_20250523.html

Europese Unie/Union européenne

▪ *Europese Commissie/Commission européenne*

15/07/25

De Europese Commissie heeft het besluit inzake de adequaatheid tussen de EU en het Europees Octrooibureau (EOB) formeel goedgekeurd. Dit is het eerste adequaatheidsbesluit dat betrekking heeft op een internationale organisatie en niet op een land of gebied. Een adequaatheidsbesluit is een besluit dat door de Europese Commissie wordt genomen op basis van artikel 45 van de AVG, waarin wordt bepaald dat een derde land (d.w.z. een land dat niet gebonden is aan de AVG) of een internationale organisatie een passend niveau van bescherming van persoonsgegevens waarborgt. Het gevolg van het adequaatheidsbesluit is dat persoonsgegevens zonder aanvullende vereisten kunnen worden doorgegeven van organisaties die onder de AVG vallen naar het betrokken derde land of de betrokken internationale organisatie. De lijst van door de Europese Commissie vastgestelde adequaatheidsbesluiten is beschikbaar op haar website. Het EDPB had advies uitgebracht over het ontwerp-adequaatheidsbesluit van de Commissie betreffende de EOB. In zijn advies merkte het EDPB op dat het gegevensbeschermingskader van het EOB grotendeels in overeenstemming is met het gegevensbeschermingskader van de Europese Unie, ook wat betreft de rechten van betrokkenen en de algemene beginselen.

La Commission européenne a formellement approuvé la décision d'adéquation entre l'UE et l'Office européen des brevets (OEB). Il s'agit de la première décision d'adéquation concernant une organisation internationale et non un pays ou un territoire. Une décision d'adéquation est une décision adoptée par la Commission européenne sur la base de l'article 45 du RGPD, qui établit qu'un pays tiers (c'est-à-dire un pays non lié par le RGPD) ou une organisation internationale assure un niveau de protection adéquat des données personnelles. La décision d'adéquation a pour effet de permettre le transfert, sans exigences supplémentaires, de données personnelles depuis les organismes soumis au RGPD vers le pays tiers ou l'organisation internationale concernés. La liste des décisions d'adéquation adoptées par la Commission européenne est disponible sur son site web. L'EDPB avait rendu son avis sur le projet de décision d'adéquation de la Commission concernant l'OEB. Dans son avis, l'EDPB avait noté que le cadre de protection des données de l'OEB est largement aligné sur le cadre de protection des données de l'Union européenne, y compris en ce qui concerne les droits des personnes concernées et les principes généraux.

Links : https://commission.europa.eu/news-and-media/news/joint-statement-michael-mcgrath-and-antonio-campinos-president-european-patent-office-2025-07-15_en
www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-072025-regarding-european-commission-draft_fr

24/06/25

De Commissie heeft de twee adequaatheidsbesluiten voor het Verenigd Koninkrijk, waardoor persoonsgegevens vrij tussen beide entiteiten kunnen circuleren, met zes maanden verlengd tot 27 december 2025. Deze besluiten hebben zowel betrekking op verwerkingen die onder de Algemene Verordening Gegevensbescherming (AVG) vallen als op verwerkingen die onder de 'LED'-richtlijn voor strafrechtelijke doeleinden vallen. De EDPB had op 5 mei 2025 (in zijn advies 06/2025) al ingestemd met deze technische en strikt in de tijd beperkte (zes maanden) verlenging van het adequaatheidsbesluit EU-VK om de Britse regering in staat te stellen het wetsontwerp inzake het gebruik van en de toegang tot gegevens (DUA Bill), dat momenteel in behandeling is in het Lagerhuis. De EDPB verduidelijkt dat dit advies geen beoordeling is van het toekomstige Britse kader voor gegevensbescherming, maar dat de Europese Commissie en de EDPB dit kader opnieuw zullen beoordelen zodra de wetswijzigingen zijn aangenomen. Na de publicatie van de technische verlenging met zes maanden heeft de Europese Commissie op 22 juli 2025 twee ontwerpteksten gepubliceerd waarin de twee adequaatheidsbesluiten ditmaal voor zes jaar worden verlengd. Deze ontwerpteksten moeten in de loop van 2025 nog worden geanalyseerd door de EDPB en door een comité bestaande uit vertegenwoordigers van de verschillende lidstaten.

La Commission a étendu pour six mois, jusqu'au 27 décembre 2025, les deux décisions d'adéquation accordées au Royaume-Uni permettant aux données personnelles de circuler librement entre les deux entités. Ces textes concernent à la fois les traitements régis par le RGPD et ceux encadrés par la directive « LED » pour les finalités pénales. L'EDPB, de son côté, avait, le 5 mai 2025 (dans son avis 06/2025) déjà accepté cette extension technique et strictement limitée dans le temps (six mois) de la décision d'adéquation EU-UK pour permettre au gouvernement britannique d'adopter le projet de loi sur l'utilisation et l'accès aux données (*DUA Bill*), actuellement en examen à la Chambre des communes. L'EDPB précise que cet avis ne constitue pas une évaluation du futur cadre britannique de protection des données, mais que la Commission européenne et l'EDPB réévalueront ce cadre une fois

les modifications législatives adoptées. Après la publication de l'extension technique de six mois, la Commission européenne a publié en date du 22 juillet 2025 deux propositions de textes renouvelant pour six années cette fois les deux décisions d'adéquation. Ces propositions de texte doivent encore être analysées par l'EDPB et par un comité composé de représentants des différents États membres dans le courant de l'année 2025.

Links : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-062025-regarding-extension-european-commission_en

13/06/25

De Raad en het Europees Parlement hebben (eindelijk) een voorlopig akkoord bereikt over de wijzigingen in de AVG die (vanuit procedureel oogpunt) de behandeling door de verschillende gegevensbeschermingsautoriteiten en het EDPB in zogenaamde 'grensoverschrijdende' zaken moeten verbeteren. De wijzigingen hebben tot doel het proces van de behandeling van grensoverschrijdende klachten van burgers of organisaties te versnellen. De Europese medewetgevers zijn het eens geworden over regels die de administratieve procedures met betrekking tot bijvoorbeeld de rechten van klagers of de ontvankelijkheid van zaken zullen vereenvoudigen en zo de toepassing van de AVG, die sinds 25 mei 2018 van kracht is, efficiënter zullen maken. De tekst harmoniseert de criteria voor de ontvankelijkheid van grensoverschrijdende klachten en garandeert zowel klagers als betrokken organisaties het recht om te worden gehoord en de voorlopige conclusies te ontvangen voordat de definitieve beslissing wordt genomen. De onderzoekstermijnen worden vastgesteld op maximaal 15 maanden (uitbreidbaar tot 27 maanden voor complexe zaken) en 12 maanden voor eenvoudige samenwerkingsprocedures. Een mechanisme voor vroegtijdige oplossing stelt de autoriteiten in staat bepaalde dossiers te behandelen voordat de standaardprocedures waarbij andere nationale autoriteiten betrokken zijn, worden gestart. De wijzigingen moeten nog formeel worden goedgekeurd door de Raad en het Europees Parlement en worden gepubliceerd in het Publicatieblad van de Europese Unie voordat ze in werking kunnen treden.

Le Conseil et le Parlement européen sont (enfin) parvenus à un accord provisoire sur les modifications au RGPD qui devraient améliorer (d'un point de vue procédural) le traitement par les différentes autorités de protection des données et l'EDPB dans les affaires dites « transfrontalières ». Les modifications ont pour but d'accélérer le processus de traitement des plaintes transfrontalières déposées par des citoyens ou des organisations. Les colégislateurs européens se sont mis d'accord sur des règles qui simplifieront les procédures administratives relatives, par exemple, aux droits des plaignants ou à la recevabilité des affaires et rendront ainsi plus efficace l'application du RGPD, qui est en vigueur depuis le 25 mai 2018. Le texte harmonise les critères d'admissibilité des plaintes transfrontalières et garantit aux plaignants comme aux organisations concernées le droit d'être entendus et de recevoir les conclusions préliminaires avant la décision finale. Des délais d'enquête sont fixés à 15 mois maximum (extensibles à 27 mois pour les cas complexes) et à 12 mois pour les procédures de coopération simple. Un mécanisme de résolution anticipée permet aux autorités de traiter certains dossiers avant d'engager les procédures standards impliquant d'autres autorités nationales. Les modifications doivent encore être formellement approuvées par le Conseil et le Parlement européen et être publiées au *Journal officiel de l'Union européenne* avant d'entrer en vigueur.

Link : www.consilium.europa.eu/en/press/press-releases/2025/06/16/data-protection-council-and-european-parliament-reach-deal-to-make-cross-border-gdpr-enforcement-work-better-for-citizens/

▪ ***European Data Protection Board (EDPB)***

03/07/25

De EDPB heeft onlangs een technisch opleidingsdocument gepubliceerd met de titel "Fundamentele principes van veilige AI-systemen met persoonsgegevens", dat zich richt op het raakvlak tussen kunstmatige intelligentie (AI) en gegevensbescherming in het kader van de AVG. Deze gids benadrukt het belang van het integreren van gegevensbeschermingsbeginselen in het ontwerp, de ontwikkeling en de implementatie van AI-systemen. De belangrijkste onderwerpen die aan bod komen, zijn onder meer gegevensminimalisatie, transparantie, verantwoordingsplicht en het waarborgen van gedegen risicobeoordelingen voor elke verwerking van persoonsgegevens door AI-technologieën.

L'EDPB a récemment publié un document de formation technique intitulé « Principes fondamentaux des systèmes d'IA sécurisés avec des données personnelles » axé sur l'intersection de l'intelligence artificielle (IA) et de la protection des données dans le cadre du RGPD. Ce guide souligne l'importance d'intégrer les principes de protection des données dans la conception, le développement et le déploiement des systèmes d'IA. Les principaux sujets abordés comprennent la minimisation des données, la transparence, la responsabilité et la garantie d'évaluations solides des risques pour tout traitement de données personnelles par les technologies d'IA.

Link : www.edpb.europa.eu/system/files/2025-06/spe-training-on-ai-and-data-protection-technical_en.pdf

04/06/25

De EDPB heeft de definitieve versie gepubliceerd van zijn Richtsnoeren 02/2024 inzake artikel 48 van de AVG (de 'Richtsnoeren') betreffende gegevensdoorgiften aan autoriteiten van derde landen. Het belangrijkste doel van deze richtsnoeren is te verduidelijken dat uitspraken of beslissingen van autoriteiten van derde landen niet automatisch of rechtstreeks kunnen worden erkend of ten uitvoer gelegd in een EU-lidstaat. De EDPB bevestigt namelijk opnieuw dat een verzoek van een buitenlandse autoriteit op zich geen rechtsgrondslag voor de verwerking of een reden voor de doorgifte vormt. Internationale overeenkomsten kunnen zowel een rechtsgrondslag als een reden voor doorgifte bieden, ook al zouden andere rechtsgrondslagen of redenen voor doorgifte in aanmerking kunnen komen bij gebrek aan een internationale overeenkomst of wanneer die overeenkomst

geen passende waarborgen biedt. Hoewel andere grondslagen op grond van artikel 6 geschikt kunnen zijn, stelt het EDPB in zijn document dat artikel 6, lid 1, onder b), dat een rechtsgrondslag biedt wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst, door een particuliere entiteit in de EU niet kan worden aangevoerd als passende rechtsgrondslag om te voldoen aan een verzoek om doorgifte of openbaarmaking van een autoriteit van een derde land.

L'EDPB a publié la version finale de ses Lignes directrices 02/2024 sur l'article 48 du RGPD concernant les transferts de données vers les autorités de pays tiers. L'objectif principal de ces lignes directrices est de préciser que les jugements ou les décisions des autorités de pays tiers ne peuvent pas être automatiquement ou directement reconnus ou exécutés dans un État membre de l'UE. En effet, l'EDPB réaffirme qu'une demande émanant d'une autorité étrangère ne constitue pas en soi une base juridique pour le traitement ou un motif pour le transfert. Les accords internationaux peuvent prévoir à la fois une base juridique et un motif de transfert même si d'autres bases juridiques ou motifs de transfert pourraient être envisagés en l'absence d'un accord international ou lorsque cet accord ne comporte pas de garanties adéquates. Toutefois, bien que d'autres bases au titre de l'article 6 puissent convenir, l'EDPB précise, dans son document, que l'article 6.1, sous b), qui fournit une base légale lorsque le traitement est nécessaire à l'exécution d'un contrat, ne peut pas être invoqué par une entité privée dans l'UE comme base juridique appropriée pour répondre à une demande de transfert ou de divulgation émanant d'une autorité d'un pays tiers.

Link : www.edpb.europa.eu/system/files/2025-06/edpb_guidelines_202402_article48_v2_en.pdf

▪ *Hof van Justitie van de EU/Cour de justice de l'UE*

04/09/25

Het Hof van Justitie heeft de reikwijdte van het begrip 'persoonsgegevens' verduidelijkt in het kader van een doorgifte van gepseudonimiseerde gegevens aan derden. Het Hof oordeelde dat "gepseudonimiseerde gegevens niet in alle gevallen en voor elke persoon als persoonsgegevens moeten worden beschouwd". Hoewel de zaak betrekking heeft op de interpretatie van Verordening 2018/1725 (ook bekend als de AVG voor EU-instellingen), wordt aangenomen dat de redenering van het Hof van Justitie ook van toepassing is op de interpretatie van de AVG.

La Cour de justice a clarifié la portée de la notion de données à caractère personnel dans le cadre d'un transfert de données pseudonymisées à des tiers. Elle a jugé que « les données pseudonymisées ne doivent pas être considérées comme constituant, dans tous les cas et pour chaque personne, des données à caractère personnel ». Alors que l'affaire porte sur l'interprétation du règlement 2018/1725 (alias RGPD pour les institutions de l'UE), la logique de la CJUE est censée être étendue à l'interprétation du RGPD également.

Link : https://curia.europa.eu/juris/document/document.jsf?text=&docid=303863&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=17325908

03/09/25

De Franse wetgever Philippe Latombe heeft de Europese Commissie aangeklaagd vanwege haar besluit van 2023 om het EU-VS-kader voor gegevensbescherming goed te keuren. Hij voerde aan dat de overeenkomst onvoldoende waarborgen voor de vertrouwelijkheid bood vanwege de wijdverbreide verzameling van massagegevens. De heer Latombe had ook kritiek op het Amerikaanse beroepsmechanisme, omdat dit volgens hem geen onafhankelijke rechtbank was en niet voldeed aan de juridische normen van de EU. Het Gerecht wees de zaak af en oordeelde dat het besluit van de Commissie op het moment van vaststelling geldig was.

Le législateur français Philippe Latombe a poursuivi la Commission européenne pour sa décision de 2023 approuvant le cadre UE-États-Unis sur la confidentialité des données. Il a fait valoir que l'accord ne présentait pas de garanties suffisantes pour la confidentialité en raison de la collecte généralisée de données en masse. M. Latombe a également critiqué le mécanisme de recours américain, affirmant qu'il ne s'agissait pas d'un tribunal indépendant et qu'il ne respectait pas les normes juridiques de l'UE. Le tribunal a rejeté l'affaire, estimant que la décision de la Commission était valide au moment de son adoption.

Link : https://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:62023TJ0553

België/Belgique

10/06/25

De GBA heeft aangekondigd dat haar nieuwe portaal online is gegaan, waardoor organisaties hun procedures en meldingen efficiënter kunnen beheren, ondanks een vertraging als gevolg van technische problemen. Het portaal biedt momenteel twee functionaliteiten: de melding en het beheer van inbreuken op persoonsgegevens, en het beheer van DPO-dossiers (melding, verwijdering en wijziging van gegevens van functionarissen). De uitbreiding van het portaal naar burgers en de toevoeging van andere procedures zijn gepland voor 2025, met handleidingen om gebruikers te begeleiden.

L'autorité de contrôle belge (APD) a annoncé la mise en ligne de son nouveau portail permettant aux organisations de gérer plus efficacement leurs procédures et notifications, malgré un retard causé par des défis techniques. Le portail propose actuellement deux fonctionnalités : la notification et la gestion des violations de données personnelles, ainsi que la gestion des dossiers DPO (notification, retrait et modification des données des délégués). L'extension du portail aux citoyens et l'ajout d'autres procédures sont prévues courant 2025, avec des manuels d'utilisation disponibles pour accompagner les utilisateurs.

Links: https://www.gegevensbeschermingsautoriteit.be/professioneel/nieuws/2025/06/10/nieuw-portaal-beschikbaar
www.autoriteprotectiondonnees.be/professionnel/actualites/2025/06/10/le-nouveau-portail-est-disponible-

14/05/25

Het hof van beroep heeft zich uitgesproken over de zaak tussen de GBA en IAB Europe (de Belgische non-profitorganisatie die de spelers in de digitale marketing- en reclamesector op Europees niveau vertegenwoordigt), waarbij het gebruik heeft gemaakt van zijn volledige rechtsbevoegdheid. Hoewel beslissing 21/2022 van de GBA om procedurele redenen wordt vernietigd, volgt het Hof van de Markten de redenering van de GBA en bevestigt het de boete van 250.000 euro die aan IAB Europe is opgelegd. Het Hof verwerpt echter de conclusies van de GBA dat IAB Europe optreedt als (gezamenlijk) verwerkingsverantwoordelijke voor de verwerkingen die volledig in het kader van het OpenRTB-protocol worden uitgevoerd.

La Cour des marchés (cour d'appel) s'est prononcée sur l'affaire opposant l'APD à IAB Europe (l'association à but non lucratif belge qui représente les acteurs du secteur du marketing et de la publicité numérique au niveau européen), en faisant usage de sa pleine juridiction. Bien que la décision 21/2022 de l'APD soit annulée pour des raisons de procédure, la Cour des marchés suit le raisonnement de l'APD et confirme l'amende de 250 000 euros imposée à IAB Europe. La Cour rejette cependant les conclusions de l'APD selon lesquelles IAB Europe agit en tant que responsable du traitement (conjoint) pour les traitements effectués entièrement dans le cadre du protocole OpenRTB.

Link : www.autoriteprotectiondonnees.be/publications/arret-du-14-mai-2025-de-la-cour-des-marches-ar-292-disponible-en-neerlandais.pdf

Frankrijk/France

22/07/25

De CNIL heeft haar nieuwste praktische fiches over AI gepubliceerd. Alle aanbevelingen van de Franse gegevensbeschermingsautoriteit hebben betrekking op de volledige levenscyclus van een AI-project, van het verzamelen van gegevens tot de integratie ervan in de systemen van bedrijven. Ze vormen een duidelijk en operationeel kader om bedrijven te begeleiden bij de verantwoordelijke en AVG-conforme ontwikkeling van hun AI-systemen.

La CNIL a publié ses dernières fiches pratiques en matière d'IA. L'ensemble des recommandations de l'autorité de protection française vise tout le cycle de vie d'un projet IA, de la collecte des données jusqu'à leur intégration dans les systèmes des entreprises. Elles constituent un cadre clair et opérationnel pour guider les entreprises dans le développement responsable et conforme au RGPD de leurs systèmes d'IA.

Link : www.cnil.fr/fr/les-fiches-pratiques-ia

11/07/25

De CNIL heeft haar standpunt verduidelijkt over het gebruik van zogenaamde 'augmented' camera's die worden gebruikt om de leeftijd van klanten in tabakswinkels te schatten. Deze apparaten, die gebaseerd zijn op algoritmen voor kunstmatige intelligentie, scannen gezichten om te beoordelen of personen meerderjarig zijn voordat producten worden verkocht die verboden zijn voor minderjarigen. De CNIL beschouwt deze praktijk als niet in overeenstemming met de AVG, omdat zij van mening is dat deze praktijk niet noodzakelijk en niet evenredig is in het licht van de nagestreefde doeleinden. Deze analyse herinnert aan de strenge eisen die gelden voor biometrische verwerking en het gebruik van AI in de openbare ruimte.

La CNIL a précisé sa position sur l'usage de caméras dites « augmentées » utilisées pour estimer l'âge des clients dans les bureaux de tabac. Ces dispositifs, reposant sur des algorithmes d'intelligence artificielle, scannent les visages afin d'évaluer la majorité des individus avant toute vente de produits interdits aux mineurs. La CNIL considère cette pratique comme non conforme au RGPD, estimant qu'elle n'est ni nécessaire ni proportionnée au regard des finalités poursuivies. Une analyse qui rappelle les exigences strictes entourant les traitements biométriques et l'usage de l'IA dans l'espace public.

Link : www.cnil.fr/fr/cameras-augmentees-pour-estimer-lage-dans-les-bureaux-de-tabac-la-cnil-precise-sa-position

15/05/25

De CNIL heeft zojuist een boete van 900.000 euro opgelegd aan SOLOCAL MARKETING SERVICES wegens tekortkomingen op het gebied van commerciële prospectie en gegevensbescherming. Na controles in het kader van haar prioritaire thema voor 2022 heeft de autoriteit vastgesteld dat het bedrijf, dat gespecialiseerd is in het verwerven en gebruiken van gegevens van potentiële klanten, via sms en e-mail aan werving deed zonder over een geldige toestemming van de betrokken personen te beschikken. Miljoenen mensen zouden door deze praktijken zijn getroffen. Uit het onderzoek bleek dat de door de partners van SOLOCAL gebruikte verzamelformulieren misleidend waren opgesteld, met duidelijk zichtbare knoppen voor aanvaarding en moeilijk te vinden opties voor weigering. Bovendien kon het bedrijf geen bewijs leveren van de toestemming van de personen van wie de gegevens door een van zijn belangrijkste leveranciers aan het bedrijf waren doorgegeven. De CNIL heeft het bedrijf ook een bevel opgelegd om te stoppen met elektronische commerciële prospectie zonder geldige toestemming, met een dwangsom van 10.000 euro per dag vertraging na afloop van een termijn van negen maanden.

La CNIL vient de prononcer une amende de 900 000 euros contre SOLOCAL MARKETING SERVICES pour des manquements relatifs à la prospection commerciale et à la protection des données. À la suite de contrôles effectués dans le cadre de sa thématique prioritaire de 2022, l'autorité a établi que la société, spécialisée dans l'acquisition et l'utilisation de données de prospects, procédait à des opérations de démarchage par SMS et courrier électronique sans disposer d'un consentement valide des personnes concernées. Plusieurs millions d'individus auraient été impactés par ces pratiques. L'enquête a révélé que les formulaires de collecte employés par les partenaires de SOLOCAL présentaient une configuration trompeuse, avec des boutons d'acceptation visuellement mis en avant et des options de refus difficiles à repérer. Par ailleurs, la société n'a pas pu fournir la preuve du consentement des personnes dont les données lui avaient été transmises par l'un de ses principaux fournisseurs. La CNIL a aussi pro-

noncé à l'encontre de la société une injonction de cesser de procéder à des opérations de prospection commerciale par voie électronique en l'absence d'un consentement valable, assortie d'une astreinte de 10 000 euros par jour de retard à l'issue d'un délai de neuf mois.

Link : www.cnil.fr/fr/sanction-de-900-000-euros-societe-solocal-marketing-services

Polen/Pologne

21/07/25

Het Poolse bureau voor de bescherming van persoonsgegevens (UODO) heeft McDonald's Polska Sp. z o.o. een aanzienlijke administratieve boete opgelegd wegens meerdere schendingen van de AVG. De beslissing wijst op tekortkomingen in de verwerking van persoonsgegevens van werknemers, waardoor gevoelige informatie onbevoegd openbaar toegankelijk werd. Deze zaak benadrukt de gedeelde verantwoordelijkheid van gegevensbeheerders en -verwerkers voor het implementeren van solide gegevensbeschermingsmaatregelen, zoals vereist door de AVG. Bovendien heeft UODO het bedrijf een berisping opgelegd voor bijkomende niet-naleving. Tegelijkertijd heeft de gegevensverwerker, 24/7 Communication Sp. z o.o., ook verschillende boetes gekregen. Deze sancties vloeien voort uit een in 2020 gemelde inbreuk op de gegevensbescherming, die betrekking had op de dossiers van werknemers van mei 2014 tot januari 2019.

L'Office polonais de protection des données personnelles (UODO) a infligé une sanction administrative substantielle à McDonald's Polska Sp. z o.o. pour de multiples violations du RGPD. La décision met en évidence des défaillances dans le traitement des données personnelles des employés, entraînant un accès public non autorisé à des informations sensibles. Cette affaire souligne les responsabilités partagées des contrôleurs de données et des sous-traitants dans la mise en place de mesures de protection des données solides, comme l'exige le RGPD. De plus, UODO a infligé une réprimande à l'entreprise pour non-conformité supplémentaire. Parallèlement, le sous-traitant des données, 24/7 Communication Sp. z o.o., a également reçu diverses amendes. Ces sanctions découlent d'une atteinte à la protection des données signalée en 2020, qui a touché les dossiers des employés de mai 2014 à janvier 2019.

Link : https://orzeczenia.uodo.gov.pl/document/urn:ndoc:gov:pl:uodo:2020:dkn_5130_4179/content

Duitsland/Allemagne

04/07/25

De regionale rechtbank van Leipzig heeft Meta Platforms Ireland, exploitant van Facebook en Instagram, veroordeeld tot het betalen van 5.000 euro aan een gebruiker wegens schending van de AVG. De zaak had betrekking op de 'Business Tools' van Meta, die in tal van websites en applicaties zijn geïntegreerd en die systematisch de persoonsgegevens van Facebook- en Instagram-gebruikers doorgeven aan Meta, ook wanneer zij niet zijn ingelogd op hun account. Deze gegevens worden over de hele wereld verzonden, met name naar de Verenigde Staten, en gebruikt voor uitgebreide profilering en gepersonaliseerde reclame, waardoor Meta het onlinegedrag van elke persoon bijna volledig kan volgen. De Duitse rechtbank baseerde haar beslissing uitsluitend op artikel 82 van de AVG betreffende de vergoeding van immateriële schade, waarbij zij zich baseerde op de jurisprudentie van het Hof van Justitie van de Europese Unie, dat van oordeel is dat voortdurende monitoring van onlineactiviteiten een gevoel van permanente inbreuk op de privacy creëert. Gezien de omvang van de verzameling en de aanzienlijke economische waarde van de advertentieprofielen voor Meta, oordeelde de rechtbank dat de schadevergoeding hoger moest zijn dan de bedragen die gewoonlijk in het nationale recht worden toegekend. Het bedrag van 5.000 euro werd vastgesteld rekening houdend met het economische model van Meta, dat het grootste deel van zijn inkomsten haalt uit gepersonaliseerde reclame, en met de toenemende maatschappelijke perceptie van de waarde van persoonsgegevens. Het hof heeft verduidelijkt dat voor deze schadevergoeding geen bewijs van concrete en individuele schade nodig is, behalve het algemene gevoel van controleverlies en kwetsbaarheid ten aanzien van het massale gebruik van gegevens. Zich ervan bewust dat deze beslissing veel gebruikers ertoe zou kunnen aanzetten om gerechtelijke stappen te ondernemen, benadrukte het hof dat deze benadering in overeenstemming was met de doelstellingen van de AVG, die ook tot doel heeft de particuliere toepassing van het recht voor de burgerlijke rechtbanken aan te moedigen, naast het optreden van de toezichthoudende autoriteiten.

Le tribunal régional de Leipzig a condamné Meta Platforms Ireland, exploitant de Facebook et Instagram, à verser 5 000 euros à un utilisateur pour violation du RGPD. L'affaire concernait les « Business Tools » de Meta, intégrés sur de nombreux sites et applications, qui transmettent systématiquement les données personnelles des utilisateurs de Facebook et Instagram à Meta, y compris lorsque ceux-ci ne sont pas connectés à leur compte. Ces données sont envoyées dans le monde entier, notamment aux États-Unis, et exploitées pour un profilage approfondi et de la publicité personnalisée, permettant à Meta de suivre presque intégralement le comportement en ligne de chaque personne. Le tribunal allemand a fondé sa décision exclusivement sur l'article 82 du RGPD relatif à l'indemnisation des dommages immatériels, en s'appuyant sur la jurisprudence de la Cour de justice de l'Union européenne, qui estime qu'une surveillance en continu des activités en ligne crée un sentiment d'atteinte permanente à la vie privée. Compte tenu de l'ampleur de la collecte et de la valeur économique considérable des profils publicitaires pour Meta, le tribunal a jugé que l'indemnité devait dépasser les montants habituellement accordés en droit national. Le montant de 5 000 euros a été fixé en tenant compte du modèle économique de Meta, qui tire l'essentiel de ses revenus de la publicité personnalisée, ainsi que de la perception sociale croissante de la valeur des données personnelles. Le tribunal a précisé que cette réparation ne nécessitait pas la preuve d'un préjudice concret et individuel au-delà du sentiment général de perte

de contrôle et de vulnérabilité face à l'utilisation massive des données. Conscient que cette décision pourrait inciter de nombreux utilisateurs à agir en justice, il a souligné que cette approche était conforme aux objectifs du RGPD, qui vise aussi à encourager l'application privée du droit devant les juridictions civiles, au-delà de l'action des autorités de contrôle.

Link : www.medienservice.sachsen.de/medien/news/1088732

Nederland/Pays-Bas

27/05/25

De Nederlandse Autoriteit Persoonsgegevens (AP) heeft scherpe kritiek geuit op een wetswijziging inzake archieven, die tot doel heeft de centrale archieven van bijzondere rechtsgebieden (CABR) online toegankelijk te maken en die aanleiding geeft tot bezorgdheid over de bescherming van persoonsgegevens van levende personen. De AP benadrukt dat de wijziging de wettelijke bescherming van gevoelige gegevens opheft en archiefinstellingen te veel vrijheid geeft om persoonlijke informatie te publiceren. Volgens de AP moeten keuzes over het evenwicht tussen toegankelijkheid en gegevensbescherming worden gemaakt door de wetgever, en niet door archivarissen, om duidelijke en democratische kaders te waarborgen. De AP benadrukt dat de toegang tot gevoelige informatie moet worden beperkt tot onderzoekers, journalisten of naasten van slachtoffers die daar een gegronde reden voor hebben, zodat deze informatie niet zonder waarborgen online kan worden gezet. Om de gegevens te beschermen, worden concrete maatregelen voorgesteld, zoals het weglaten van persoonsgegevens in onderzoeken of het beperken van het aantal toegankelijke registraties per dag. De minister, die adviezen ontvangt van verschillende instanties, waaronder het Adviescomité voor toegang van het publiek tot en beheer van informatie, dat eveneens kritisch is, moet het wetsontwerp ter advies voorleggen aan de Raad van State.

L'autorité de contrôle néerlandaise (AP) a vivement critiqué un projet de modification de la loi sur les archives, motivé par la volonté de rendre accessibles en ligne les archives centrales des juridictions spéciales (CABR), et qui suscite des inquiétudes quant à la protection des données personnelles des personnes vivantes. L'AP souligne que la modification supprime la protection juridique des données sensibles et laisse une trop grande liberté aux institutions d'archives pour publier des informations personnelles. Selon elle, les choix concernant l'équilibre entre accessibilité et protection des données doivent relever du législateur, et non des archivistes, afin de garantir des cadres clairs et démocratiques. L'AP insiste sur la nécessité de restreindre l'accès aux informations sensibles aux seuls chercheurs, journalistes ou proches de victimes ayant une raison valable, excluant ainsi toute mise en ligne sans garanties. Pour protéger les données, des mesures concrètes comme l'omission des données personnelles dans les recherches ou la limitation du nombre d'enregistrements accessibles par jour sont proposées. Le ministre, recevant des avis de divers organismes, dont le Comité consultatif sur l'accès du public et la gestion de l'information, également critique, doit soumettre le projet de loi au Conseil d'État pour avis.

Link : https://autoriteitpersoonsgegevens.nl/actueel/wetsvoorstel-over-archieven-gaat-te-ver

23/05/25

De AP heeft haar visie op de verantwoorde ontwikkeling en implementatie van generatieve AI gedeeld. Deze visie geeft een beeld van de technologie, bespreekt trends, schetst toekomstscenario's en bevat verschillende juridische interpretaties. De AP had organisaties uitgenodigd om tot 27 juni 2025 hun mening te geven over deze voorlopige visie.

L'AP a partagé sa vision sur le développement et le déploiement responsables de l'IA générative. Cette vision donne une image de la technologie, commente les tendances, esquisse des scénarios futurs et contient plusieurs interprétations juridiques. L'AP avait invité les organisations à donner leur avis sur cette vision préliminaire jusqu'au 27 juin 2025.

Link : https://autoriteitpersoonsgegevens.nl/actueel/ap-gezamenlijke-keuzes-nodig-voor-verantwoorde-inzet-generatieve-ai

Agenda

- 27 November 2025 @ 12:30 AM
  Webinar "Aperçu actua" (FR)
  Jacques Folon
- 4 December 2025 @ 4:00 PM
  Webinar "Qualificatie werknemers en vergelijkbare statuten onder de AVG" (NL)
  Johan Vandendriessche
- 11 December 2025 @ 4:00 PM
  Webinar "Quantum Computing" (EN)
  Deborah Nas

Jurisprudence

La protection contre le licenciement du DPO

Commentaire du jugement du tribunal du travail francophone de Bruxelles du 17 mai 2024[1]

Introduction

C'est la première fois, à notre connaissance, qu'une juridiction du travail belge a à se prononcer sur le licenciement d'un délégué à la protection des données (« DPO[2] »).

Le jugement rendu par le tribunal du travail francophone de Bruxelles le 17 mai 2024 à ce sujet nous permet de nous interroger sur la limite posée par l'article 38, § 3, du RGPD, lequel interdit le « relèvement » des fonctions d'un DPO pour un motif tiré de « l'exercice de ses missions », lesquelles comprennent le contrôle du respect des dispositions en matière de protection des données ainsi que des règles internes de l'employeur en matière de protection des données à caractère personnel.

Plus particulièrement, il nous amène à questionner la portée réelle de la protection contre le licenciement du DPO. Cette protection est-elle une interdiction absolue de licenciement ou se veut-elle être une interdiction simplement relative ?

Après avoir rappelé les faits et la décision rendue par le tribunal du travail dans cette affaire (I et II), nous examinerons la portée exacte de la protection contre le licenciement du DPO à la lumière du jugement commenté et, plus largement mais pas uniquement, de la jurisprudence européenne sur la question (III).

I. Faits — Un licenciement partiellement fondé sur la fonction de DPO

Un travailleur occupé en qualité de « Chief information security officer / Data privacy officer » dans les liens d'un contrat de travail à durée indéterminée[3] auprès d'un hôpital depuis près de cinq ans est licencié moyennant paiement de l'indemnité compensatoire de préavis légale.

Estimant que son licenciement est fondé sur l'exercice de ses missions de délégué à la protection des données, en violation de l'interdiction prévue par l'article 38, § 3, du RGPD[4] de relever de ses fonctions un délégué à la protection des données pour l'exercice de ses fonctions[5], le travailleur sollicite une indemnité évaluée *ex aequo et bono* à trois mois de rémunération, outre une demande d'indemnité pour licenciement manifestement déraisonnable de 17 semaines de rémunération basée sur la CCT n° 109[6] (abordée au point II ci-après).

L'hôpital invoque quant à lui que les motifs du licenciement ne sont pas liés à l'essence même de la fonction de DPO, mais qu'ils ont davantage trait à un manque de communication claire de la part du travailleur et des difficultés de compréhension mutuelle.

Tant la proposition de licenciement que le courrier de licenciement font en effet état de difficultés dans le chef du travailleur à faire comprendre ses besoins et à être pédagogique, à proposer des éléments concrets et des solutions ou des pistes de solutions, d'une posture de « conseiller » uniquement, poussée à l'extrême, d'une approche extrêmement théorique et peu traduite en éléments pratiques et concrets, de difficultés à transposer ses souhaits théoriques en un *work flow* pratique, de difficultés à produire du rédactionnel de qualité, accessible et compréhensible, d'une certaine désorganisation et « approche brouillonne », d'un manque de rigueur, d'une perception de son rôle trop limitative par rapport aux attentes, aux besoins et au profil de fonction et d'une incapacité à travailler avec certains secteurs comme par exemple le service IT.

Selon le tribunal, conformément à l'article 8.3 du Code civil, l'employeur a la charge de la preuve du fait que le délégué à la protection des données a été licencié pour un motif étranger à ses missions.

Le tribunal relève que les reproches formulés par l'hôpital concernent indistinctement la fonction de *Chief information security officer* et de *Data privacy officer* pour les motifs suivants :

- Les responsabilités étaient partagées, la proposition de licenciement ajoutant que les responsabilités n'incombaient pas seulement au travailleur mais à l'hôpital et faisant état d'un faible niveau de maturité de l'organisation concernant les problématiques liées à la documentation de processus avec une culture très informelle, d'un manque d'intérêt ou de priorisation des sujets en lien avec le RGPD, de la gestion du Covid depuis mars 2020 et d'un manque de compréhension des attentes et des besoins du travailleur pour avancer concrètement et de concert.
- La proposition de licenciement reconnaît que l'hôpital a accordé la priorité à la fonction de *Chief information security officer* en minimisant l'intérêt pour la fonction de *Data privacy officer* car il s'agissait d'un rôle nouveau rendu nécessaire par l'arrivée de la législation sur le RGPD.
- Dans la lettre de licenciement, l'hôpital reproche au travailleur de se positionner comme un conseiller formulant des recommandations mais agissant peu. Ses conseils seraient très théoriques et il ne proposerait pas d'axes de mise en œuvre concrets.

Selon le tribunal, l'hôpital reproche au travailleur le fait que sa seconde fonction de DPO ne lui a pas permis d'exer-

[1] Trib. trav. fr. Bruxelles (1re ch.), 17 mai 2024, R.G. n° 23/853/A, www.terralaboris.be.

[2] « *Data Protection Officer* » ou « Délégué à la protection des données » selon les termes du RGPD.

[3] Il est permis, aux termes de l'article 37, § 6, du RGPD, de cumuler la fonction de délégué à la protection des données avec une autre fonction pour autant que les missions et tâches en question n'entraînent pas de conflit d'intérêts.

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L 119, 4 mai 2016.

[5] « Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. »

[6] Il est en réalité question d'une demande fondée sur un abus de droit de licenciement dans le secteur public appréciée à l'aune de la CCT n° 109 dont les juridictions devaient s'inspirer dans l'attente de l'adoption d'une législation comparable à la CCT n° 109 (finalement entrée en vigueur le 1er mai 2024 à la suite de l'adoption de la loi du 13 mars 2024 sur la motivation des licenciements et des licenciements manifestement déraisonnables des travailleurs contractuels du secteur public).

cer comme l'hôpital le souhaitait sa première fonction de *Chief information security officer*. Le tribunal considère que, ce faisant, l'hôpital n'établit pas que le licenciement n'est fondé que sur l'exercice de la première fonction de *Chief information security officer*.

II. Décision — Une indemnité pour violation de l'interdiction de licenciement du DPO évaluée *ex aequo et bono* mais pas d'indemnité pour licenciement manifestement déraisonnable

Compte tenu de ce qui précède, le tribunal estime que le licenciement du travailleur viole l'interdiction établie par l'article 38, § 3, du RGPD.

Aucune sanction n'étant prévue par le RGPD ou le droit belge, le tribunal évalue le dommage du travailleur *ex aequo et bono* à trois mois de rémunération, indemnité que le tribunal estime raisonnable. Le tribunal souligne néanmoins qu'il est « tenu » par l'évaluation de trois mois demandée par le travailleur, évaluation qui reste, comme le tribunal le souligne, bien éloignée des montants forfaitaires prévus par d'autres législations (trois à six mois contre l'auteur d'un harcèlement, six mois en cas de licenciement en raison d'un mandat politique ou par la suite d'un harcèlement, ou en cas de discrimination, plusieurs années en ce qui concerne les délégués syndicaux ou les conseillers en prévention). Ce faisant, le tribunal semble sous-entendre que le travailleur aurait pu songer à réclamer un montant supérieur à trois mois de rémunération.

Concernant la demande d'indemnité pour licenciement manifestement déraisonnable ou abusif de 17 semaines de rémunération, le tribunal constate que le licenciement est fondé sur l'aptitude et la conduite de l'intéressé : il n'a produit que dix textes en quatre ans ; il ne s'est occupé du registre des traitements qu'en 2018 et 2019 ; dans son état des lieux des tâches effectuées remis en 2022, la majeure partie d'entre elles a été effectuée en 2019 et 2020 ; il n'a pas signalé l'existence d'un registre des incidents liés au traitement des données et n'a pas complètement rempli celui-ci. Le tribunal va donc rejeter cette demande, estimant que tout employeur prudent et raisonnable confronté à une telle situation aurait envisagé un licenciement.

III. La portée de la protection contre le licenciement du DPO — Une interdiction de licenciement relative et non absolue

A. Rôle du DPO

Le délégué à la protection des données doit obligatoirement être désigné lorsque le traitement est effectué par une autorité publique ou un organisme public, ou lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ou qu'elles consistent en un traitement à grande échelle de catégories particulières de données[7].

Il doit être associé à toutes les questions relatives à la protection des données à caractère personnel[8]. Ses missions sont au moins les suivantes :

- informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en matière de protection des données ;
- contrôler le respect des dispositions en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;
- dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ;
- coopérer avec l'autorité de contrôle ;
- faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement et mener des consultations, le cas échéant, sur tout autre sujet[9].

B. Indépendance fonctionnelle du DPO et protection contre le licenciement du DPO

Le délégué à la protection des données, qu'il soit ou non un employé du responsable du traitement[10], devrait être en mesure d'exercer ses fonctions et missions en toute indépendance[11]. À cet égard, une telle indépendance doit nécessairement lui permettre d'exercer ses missions conformément à l'objectif du RGPD, qui vise notamment à assurer un niveau élevé de protection des personnes physiques au sein de l'Union et, à cette fin, à assurer une application cohérente et homogène des règles de protection des libertés et des droits fondamentaux de ces personnes à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union[12]. Il est ainsi soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions[13].

Pour préserver cette indépendance « fonctionnelle » du délégué, l'article 38, § 3, du RGPD fixe une limite qui consiste à interdire de relever de sa fonction un délégué ainsi que toute forme de pénalisation d'un délégué pour un motif tiré de l'exercice de ses missions[14] :

> « 3. Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant. »

Selon la Cour de justice de l'Union européenne, ceci signifie que le délégué doit être protégé contre toute décision

[7] Art. 37, § 1er, du RGPD.

[8] Art. 38, § 1er, du RGPD.

[9] Art. 39, § 1er, du RGPD.

[10] « Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service » (Art. 37, § 6, du RGPD). .

[11] Considérant 97 du RGPD.

[12] C.J.U.E., arrêt *Leistritz AG c. LH*, 22 juin 2022, C-534/20, EU:C:2022:495, point 26.

[13] Art. 38, § 5, du RGPD.

[14] C.J.U.E., arrêt *Leistritz AG c. LH* précité, point 25.

par laquelle il serait mis fin à ses fonctions, par laquelle il subirait un désavantage ou qui constituerait une sanction[15]. Est susceptible de constituer une telle décision une mesure de licenciement d'un délégué à la protection des données qui serait prise par son employeur et qui mettrait fin à la relation de travail existant entre ce délégué et cet employeur ainsi que, partant, également à la fonction de délégué à la protection des données au sein de l'entreprise concernée[16].

La Cour de justice précise que l'article 38, § 3, deuxième phrase, du RGPD n'a, en revanche, pas pour objet de régir globalement les relations de travail entre un responsable du traitement ou un sous-traitant et des membres de son personnel, lesquelles ne sont susceptibles d'être affectées que de manière accessoire, dans la mesure strictement nécessaire à la réalisation des objectifs de préservation de l'indépendance fonctionnelle du délégué et de garantie de l'effectivité des dispositions du RGPD[17].

En effet, la fixation des règles relatives à la protection contre le licenciement d'un délégué relève du domaine de la politique sociale à l'égard de laquelle l'Union et les États membres disposent d'une compétence partagée. Ainsi, les États membres peuvent prévoir des dispositions particulières plus protectrices en matière de licenciement du délégué à la protection des données pour autant que ces dispositions soient compatibles avec le droit de l'Union et les dispositions du RGPD (en particulier son article 38, § 3, deuxième phrase)[18].

Une telle protection, précise la Cour, ne saurait toutefois compromettre la réalisation des objectifs du RGPD. Or, tel serait le cas si celle-ci empêchait tout licenciement d'un délégué à la protection des données qui ne posséderait plus les qualités professionnelles requises pour exercer ses missions ou qui ne s'acquitterait pas de celles-ci conformément aux dispositions du RGPD[19]. Tel serait également le cas selon la Cour si cette protection empêchait toute révocation d'un délégué dans l'hypothèse où il ne serait pas ou plus en mesure d'exercer ses tâches en toute indépendance en raison de l'existence d'un conflit d'intérêts qui compromettrait la réalisation des objectifs précités du RGPD[20].

La Cour conclut donc en précisant que l'article 38, § 3, deuxième phrase, du RGPD ne s'oppose pas à une réglementation nationale comme le droit allemand qui prévoit qu'un délégué ne peut être licencié que pour un motif grave, même si ce licenciement n'est pas lié à l'exercice des missions de ce délégué « pour autant qu'une telle réglementation ne compromette pas les objectifs du RGPD »[21].

C. Réflexions sur la protection contre le licenciement du DPO

Selon le tribunal du travail francophone de Bruxelles, le droit belge ne prévoit pas de dispositions particulières en matière de licenciement du délégué à la protection des données. Le tribunal en déduit que, dès l'instant où une décision de licenciement se fonde — même partiellement — sur l'exercice des fonctions de DPO, elle viole l'interdiction de licenciement prescrite par l'article 38 précité. On serait même tenté d'ajouter que le tribunal considère que, même si une décision de licenciement se fonde — légitimement — sur l'exercice des fonctions de DPO, elle viole l'interdiction prévue par cet article. En effet, lorsqu'il a analysé la question de savoir si le licenciement était manifestement déraisonnable ou abusif, le tribunal a considéré que les motifs de licenciement, tous tirés des tâches (mal exécutées) de DPO, étaient raisonnables et légitimes. À suivre le tribunal, il serait donc impossible de licencier un DPO pour des raisons liées à l'exercice de ses missions de DPO, même en cas de dysfonctionnement avéré dans l'exercice de telles missions. Il faudrait, dans tous les cas, exclusivement motiver la décision de licenciement par une raison totalement étrangère à l'exercice (même insatisfaisant) des fonctions de DPO (par exemple, des dysfonctionnements constatés dans l'exercice d'une autre fonction qu'exercerait le DPO pour l'employeur).

Un tel raisonnement ne va-t-il pas précisément à l'encontre des objectifs du RGPD, étant « d'assurer un niveau élevé de protection des personnes physiques au sein de l'Union et, à cette fin, à assurer une application cohérente et homogène des règles de protection des libertés et des droits fondamentaux de ces personnes à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union » ? Est-il réellement porté atteinte à l'indépendance fonctionnelle du délégué lorsqu'une décision de licenciement se fonde sur la manière (problématique) dont il exerce ses fonctions de DPO ? Le licenciement s'appuie, certes, sur des motifs liés à l'exercice des missions de délégué, mais avant tout parce qu'il est « incompétent » dans l'exercice de ses missions. Il n'y a, de ce fait, pas atteinte à l'indépendance du délégué (on ne le licencie pas en raison d'un avis qu'il a donné au sujet d'un traitement particulier susceptible d'engendrer un risque élevé nécessitant une analyse d'impact relative à la protection des données, par exemple[22]), mais constat d'une inaptitude ou d'une incompétence à exercer ses missions de délégué. Autrement dit, on ne licencie pas le délégué *en raison* de l'exercice de ses missions mais *en raison* de l'exercice *incorrect* de ses missions.

[15] Le Groupe de travail « Article 29 » sur la protection des données indique à ce sujet : « Les sanctions peuvent prendre des formes diverses et peuvent être directes ou indirectes. Il peut s'agir, par exemple, d'absence de promotion ou de retard dans la promotion, de freins à l'avancement de carrière ou du refus de l'octroi d'avantages dont bénéficient d'autres travailleurs. Il n'est pas nécessaire que ces sanctions soient effectivement mises en œuvre, une simple menace suffit pour autant qu'elle soit utilisée pour sanctionner le DPD [Délégué à la protection des données] pour des motifs liés à ses activités de DPD » (Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices concernant les délégués à la protection des données (DPD)*, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 18). Depuis l'entrée en vigueur du RGPD, ce groupe de travail a été remplacé par le Comité européen de la protection des données (CEPD). Celui-ci a approuvé les lignes directrices sur les DPD au cours de sa première assemblée plénière, le 25 mai 2018 (voy. https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf).

[16] C.J.U.E., arrêt *Leistritz AG c. LH* précité, points 21 et 22. Dans le même sens : C.J.U.E., arrêt *ZS c. Zweckverband « Kommunale Informationsverarbeitung Sachsen » KISA, Körperschaft des öffentlichen Rechts*, 9 février 2023, C-560/21, ECLI:EU:C:2023:81, points 16 et 17 ; C.J.U.E., arrêt *X-FAB Dresden GmbH & Co. KG c. FC*, 9 février 2023, C-453/21, EU:C:2023:79, points 21 et 22.

[17] C.J.U.E., arrêt *Leistritz AG c. LH* précité, point 28.

[18] C.J.U.E., arrêt *Leistritz AG c. LH* précité, points 31 à 34. Dans le même sens : C.J.U.E., arrêt *ZS c. Zweckverband « Kommunale Informationsverarbeitung Sachsen » KISA, Körperschaft des öffentlichen Rechts* précité, point 26 ; C.J.U.E., arrêt *X-FAB Dresden GmbH & Co. KG c. FC* précité, point 31.

[19] C.J.U.E., arrêt *Leistritz AG c. LH* précité, point 35. Dans le même sens : C.J.U.E., arrêt *ZS c. Zweckverband « Kommunale Informationsverarbeitung Sachsen » KISA, Körperschaft des öffentlichen Rechts* précité, point 27 ; C.J.U.E., arrêt *X-FAB Dresden GmbH & Co. KG c. FC* précité, point 32.

[20] C.J.U.E., arrêt *ZS c. Zweckverband « Kommunale Informationsverarbeitung Sachsen » KISA, Körperschaft des öffentlichen Rechts* précité, point 29. Dans le même sens : C.J.U.E., arrêt *X-FAB Dresden GmbH & Co. KG c. FC* précité, point 34.

[21] C.J.U.E., arrêt *Leistritz AG c. LH* précité, point 36.

[22] Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices concernant les délégués à la protection des données (DPD)*, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 18.

Il est vrai que le Groupe de travail « Article 29 » semblait n'envisager que des hypothèses de licenciement pour des circonstances tout à fait étrangères à l'exercice des missions : « [d]ans le cadre d'une gestion normale, et comme c'est le cas pour tout autre employé ou sous-traitant conformément au droit des contrats ou au droit du travail et au droit pénal applicables au niveau national, et selon les conditions qui y sont fixées, un DPD[23] pourra toujours être licencié légitimement pour des motifs autres que l'exercice de ses missions de DPD (par exemple, en cas de vol, de harcèlement physique, moral ou sexuel ou d'autres fautes graves similaires) »[24].

On s'interroge toutefois, avec Karen Rosier, sur la possibilité de licencier un délégué médiocre, incompétent, faisant preuve d'un manque de proactivité ou commettant des erreurs d'appréciation[25].

La Cour de justice précise en effet qu'en « empêchant » tout licenciement d'un délégué à la protection des données qui « ne posséderait plus les qualités professionnelles requises pour exercer ses missions ou qui ne s'acquitterait pas de celles-ci conformément aux dispositions du RGPD », la réalisation des objectifs du RGPD serait mise à mal. Il en serait selon nous ainsi dans l'hypothèse où un employeur serait contraint de continuer à occuper son délégué à la protection des données en dépit des manquements constatés dans l'exercice de ses missions de délégué.

Dans ses conclusions précédant l'arrêt *Leistritz*, l'avocat général, rejoint par la Cour de justice, indiquait, dans un même ordre d'idées :

> « 50. Cependant, l'interdiction énoncée à l'article 38, paragraphe 3, deuxième phrase, du règlement 2016/679 a nécessairement des limites en cas de dysfonctionnements objectifs dans l'exercice des missions du délégué à la protection des données eu égard à ses obligations. Ces limites doivent être fixées en conformité avec l'objectif poursuivi par ce règlement.
>
> 51. Ainsi, une interprétation tout aussi conforme à l'objectif du règlement 2016/679 doit conduire, selon moi, à admettre qu'un délégué à la protection des données puisse être relevé de ses fonctions lorsqu'il ne répond plus aux critères qualitatifs nécessaires à l'exercice de ses missions, tels que ceux énoncés à l'article 37, paragraphe 5, de ce règlement, ou ne satisfait pas aux obligations fixées à l'article 38, paragraphe 3, première et troisième phrases, ainsi que paragraphes 5 et 6, dudit règlement ou encore lorsque son niveau d'expertise s'avère insuffisant. » [26]

Cette position est en accord avec la position de l'autorité belge de protection des données, qui considère que le délégué à la protection des données peut être licencié pour des raisons étrangères à sa fonction de délégué ou s'il ne possède plus les qualités professionnelles requises pour exercer ses missions :

> « Le délégué à la protection des données ne peut pas être licencié pour des motifs liés à l'exercice de sa fonction de délégué. Ceci ne signifie pas que le délégué est "intouchable". Il peut être licencié dans le respect des dispositions légales nationales applicables en droit des contrats, en droit du travail ou de droit pénal, par exemple. Il pourrait être mis fin à la fonction du délégué pour des motifs légitimes, en cas de vol, harcèlement ou faute grave similaire. La Cour de Justice de l'Union européenne a décidé dans son arrêt dans l'affaire C-534/20 du 22 juin 2022 que *le DPO peut être licencié s'il ne possède plus les qualités professionnelles requises pour exercer ses missions ou s'il ne s'acquitte pas de ses missions conformément aux dispositions du RGPD*. Cependant le délégué ne peut pas être licencié en raison d'un conseil qu'il aurait donné en matière de protection des données, en raison de la détection et du signalement d'un manquement du responsable de traitement ou du sous-traitant à l'une de leurs obligations en matière de protection des données ou de sa coopération avec l'autorité de contrôle, par exemple. Le délégué ne peut pas non plus être pénalisé en raison de l'exercice de sa fonction. Il ne peut par exemple être pénalisé dans son parcours de carrière dans l'entreprise pour des motifs liés à l'exercice de sa fonction, voir son avancement retardé ou se voir refuser des avantages que d'autres employés reçoivent. La simple menace de telles sanctions suffit sans qu'il soit besoin qu'elles soient effectivement mises en œuvre. »[27]

En France, la CNIL, la Commission nationale de l'informatique et des libertés, en fait mention elle aussi dans son Guide pratique RGPD — Délégués à la protection des données :

> « [Le DPO] peut, comme tout autre salarié ou agent, être licencié pour des motifs autres que l'exercice de ses missions de délégué, par exemple en cas de vol, de harcèlement moral ou d'autres fautes graves similaires. Enfin, l'organisme qui désigne un DPO doit s'assurer que ce dernier détient les qualifications et les capacités lui permettant d'accomplir ses missions. Il peut dès lors décider de retirer les missions de DPO à un salarié n'étant pas à même de remplir les missions qui lui sont attribuées par le RGPD. Cette procédure n'est possible que si l'employeur s'est assuré que la difficulté du DPO à assurer ses missions ne vient pas d'une insuffisance des moyens — notamment temporels — qui lui sont accordés. »[28]

Toujours en France, le Conseil d'État a, par un arrêt du 21 octobre 2022, au sujet du licenciement d'une déléguée à la protection des données, considéré que « en estimant que l'exigence de protection de l'indépendance fonctionnelle du délégué à la protection des données ne faisait pas obstacle, par principe, à ce que la société […] puisse reprocher à l'intéressée [déléguée à la protection des données] des carences dans l'exercice de ses fonctions ainsi que le non-respect de règles internes à la société, dont il n'est pas allégué qu'elles étaient incompatibles avec l'indépendance fonctionnelle du délégué, la CNIL n'a pas commis d'erreur de droit. Par ailleurs, eu égard aux justifications avancées par la société […] pour motiver les mesures prises à l'égard de Mme C., et quand bien même la matérialité de certains des faits reprochés à cette dernière

[23] Délégué à la protection des données.

[24] Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices concernant les délégués à la protection des données (DPD)*, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 19.

[25] K. Rosier, « Délégué à la protection des données : une nouvelle fonction, un métier en devenir », *in* B. Docquir (dir.), *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, p. 160.

[26] Av. gén. J. Richard De La Tour, concl. préc. C.J.U.E., arrêt *Leistritz AG c. LH* précité, points 50 et 51.

[27] https://www.autoriteprotectiondonnees.be (nous mettons en évidence).

[28] www.cnil.fr.

ne serait pas établie avec certitude, il ne ressort pas des pièces du dossier que la CNIL, dans l'exercice du large pouvoir d'appréciation qui est le sien, ait entaché sa décision d'une erreur manifeste en estimant qu'il n'y avait pas lieu, en l'espèce, d'engager des poursuites à l'encontre de la société [...] à raison d'un manquement au paragraphe 3 de l'article 38 du RGPD »[29]. Le Conseil d'État a, par conséquent, rejeté la demande d'annulation de la décision de la CNIL de clôturer la plainte de la déléguée relative aux conditions dans lesquelles elle a exercé ses fonctions de déléguée au sein de cette société et à l'exercice de son droit d'accès à ses données personnelles.

Interprétée comme n'interdisant que le licenciement en représailles à l'exercice légitime de ses missions, la protection contre le licenciement du délégué à la protection des données n'est pas sans rappeler celle du conseiller en prévention. Elle n'est pas non plus sans faire penser à une protection moins connue, celle de conseiller en sécurité et en protection de la vie privée dans les zones de police, qui ne peut être écarté de ses fonctions que pour des motifs qui sont étrangers à son indépendance ou pour des motifs qui démontrent qu'il est incompétent à exercer ses missions[30].

Tout comme le délégué à la protection des données, le conseiller en prévention (interne) est chargé de différentes missions au sein de l'entreprise (liées au bien-être des travailleurs) qui requièrent une indépendance et une protection contre toute forme de représailles à l'exercice de ses missions. Il s'agit, ici aussi, d'une protection dite « fonctionnelle », à savoir une protection reconnue au travailleur au regard des fonctions qu'il exerce soit au sein de l'entreprise (conseiller en prévention d'un service interne de prévention et de protection au travail) ou en dehors de l'entreprise (conseiller en prévention d'un service externe de prévention et de protection au travail)[31]. Le conseiller en prévention ne peut, selon la loi du 20 décembre 2002, être licencié « que pour des motifs qui sont étrangers à son indépendance ou pour des motifs qui démontrent qu'il est incompétent à exercer ses missions et pour autant que les procédures visées par la [...] loi soient respectées »[32].

Selon les travaux préparatoires de la loi du 20 décembre 2002, « la notion de compétence doit être interprétée en fonction de la formation de base et la formation complémentaire dont le conseiller en prévention dispose, ainsi qu'en fonction de son expérience. En outre, il existe une relation entre la compétence du conseiller en prévention et les compétences qui doivent être présentes dans l'entreprise, afin de pouvoir mener à bon terme la politique de prévention et l'exécution du plan global de prévention »[33].

L'incompétence invoquée doit porter sur l'exercice des missions dévolues au conseiller en prévention[34]. Il reste toutefois possible de licencier un conseiller en prévention pour des motifs liés aux autres tâches confiées au conseiller en prévention dans le cadre du contrat de travail, dans la mesure où elles sont étrangères à son indépendance[35].

Les conseillers en prévention doivent également pouvoir exercer leurs fonctions en toute indépendance. Ils ne peuvent subir de préjudice en raison de leurs activités en tant que conseillers en prévention[36]. Au sujet de l'indépendance des conseillers en prévention, les travaux préparatoires de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail indiquent : « Cet article comporte une disposition fondamentale concernant les conseillers en prévention. Ils doivent remplir leur mission en toute indépendance à l'égard de l'employeur et des travailleurs. Cette règle est essentielle afin qu'ils puissent remplir leur devoir de conseiller expert tant à l'égard de l'employeur qu'à l'égard des travailleurs. C'est pourquoi l'exercice de cette mission ne peut pas davantage comporter un préjudice pour eux »[37].

Les travaux préparatoires de la loi du 20 décembre 2002 explicitent la notion d'indépendance du conseiller en prévention de la manière suivante : « la notion d'indépendance doit être interprétée sous l'angle de l'exercice de la fonction. Cela veut dire qu'elle a les caractéristiques suivantes :

- la liberté pour le conseiller en prévention de choisir, sur base de sa formation, les moyens nécessaires afin de pouvoir donner des avis fondés en matière de prévention ;
- le droit de recevoir des informations ;
- la liberté de donner des avis objectifs qui ne tiennent, dès lors, pas nécessairement compte des intérêts différents de l'employeur et des travailleurs, mais qui ont pour objectif de servir l'intérêt général, dans le cas présent, le bien-être au travail. »[38]

Autrement dit, ils ne peuvent être licenciés en représailles à l'exercice de leur mission ou pour les empêcher d'exercer leurs missions[39].

La loi de 2002 ne vise donc pas à empêcher tout licenciement du conseiller en prévention mais à régler les deux hypothèses dans lesquelles il peut être licencié. Un conseiller en prévention peut donc bien être licencié pour des raisons liées à l'exercice de sa fonction pour autant que les raisons invoquées soient étrangères à son indépendance ou qu'il soit démontré qu'il est incompétent à exercer sa fonction. Lorsque la procédure de licenciement

[29] Arrêt n° 459254 disponible sur https://www.conseil-etat.fr.

[30] Art. 6, al. 3, de l'A.R. du 6 décembre 2015 relatif aux conseillers en sécurité et en protection de la vie privée et à la plate-forme de la sécurité et de la protection des données, *M.B.*, 28 décembre 2015. Dans le Rapport au Roi précédant l'arrêté royal, il est ainsi indiqué : « Le conseiller en sécurité et en protection de la vie privée et ses collaborateurs éventuels ne peuvent pas être relevés de leur fonction en raison des avis qu'ils émettent ou des actes qu'ils accomplissent dans le cadre de l'exercice normal de leurs fonctions. Cet article s'inspire de l'article 3 de la loi du 20 décembre 2002 portant protection des conseillers en prévention. [...] Afin de préserver son indépendance, le conseiller doit pouvoir être proche du haut management à qui il s'adresse directement. Il ne peut pas subir de désavantage dans sa carrière en raison de l'accomplissement de ses missions. Il peut toutefois être déchargé de ses fonctions par l'autorité compétente dès lors qu'il manque gravement aux devoirs de sa mission ».

[31] C. Broucke, M.-C. Paternostre et F. Verbrugge, « Les protections contre le licenciement : essai de synthèse 2.0 (partie I/II) », *Ors.*, 2024/11, p. 12.

[32] Art. 3 de la loi du 20 décembre 2002 portant protection des conseillers en prévention, *M.B.*, 20 janvier 2003.

[33] Projet de loi portant protection des conseillers en prévention, Exposé des motifs, *Doc. parl.*, Ch., 2001-2002, n^{os} 50-2032/001 et 50-2033/001, p. 17.

[34] C. trav. Mons (1re ch.), 24 février 2017, R.G. n° 2016/AM/366, www.terralaboris.be.

[35] J. Vanthournout, *Praktijkgids. De bescherming van de preventieadviseur*, Anvers, Standaard Uitgeverij, 2003, p. 116, n° 134.

[36] Art. 43 de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail, *M.B.*, 18 septembre 1996. Une disposition similaire est prévue dans le Code du bien-être au travail (art. II.1-24).

[37] Projet de loi concernant le bien-être des travailleurs lors de l'exécution de leur travail, Exposé des motifs, *Doc. parl.*, Ch., 1995, n° 71/1, p. 28.

[38] Projet de loi portant protection des conseillers en prévention, Exposé des motifs, *Doc. parl.*, Ch., 2001-2002, n^{os} 50-2032/001 et 2033/001, p. 16.

[39] J. Vanthournout, *Praktijkgids. De bescherming van de preventieadviseur*, *op. cit.*, p. 115, n° 132.

n'est pas respectée ou qu'il a été porté atteinte à l'indépendance du conseiller en prévention ou que les motifs invoqués en ce qui concerne l'incompétence à exercer ses missions ne sont pas prouvés, l'employeur sera redevable d'une indemnité de protection[40].

Nous pensons qu'en interdisant à l'employeur de mettre fin au contrat de travail du délégué à la protection des données pour l'exercice de ses missions, le législateur européen, comme le législateur belge vis-à-vis du conseiller en prévention et du conseiller en sécurité, a avant tout voulu protéger le délégué contre toute décision de licenciement qui porterait atteinte à son indépendance, c'est-à-dire, en représailles à l'exercice légitime de ses tâches. Le délégué à la protection des données ne peut en effet subir aucune mesure préjudiciable en raison de l'exercice « normal » de ses fonctions de délégué.

Un licenciement décidé en raison de l'incompétence avérée du délégué à exercer ses missions ne violerait pas, selon nous, cette interdiction. De même, un licenciement pour des motifs totalement étrangers à l'exercice de sa fonction de délégué (problèmes de comportement, dysfonctionnements dans l'exercice d'une autre fonction que celle de délégué, motif économique, etc.) ne serait pas plus critiquable au regard de l'article 38, § 3, du RGPD.

Conclusion

L'interdiction de licenciement prévue par l'article 38, § 3, du RGPD n'est, à notre estime, pas une interdiction pure et simple de licenciement mais une interdiction de licenciement du délégué pour un motif qui porterait atteinte à l'indépendance fonctionnelle du délégué.

Violerait une telle interdiction un licenciement qui serait décidé en représailles à un incident soulevé par un délégué en matière de violation de la protection des données à caractère personnel ou en raison de recommandations légitimes en matière de protection des données. L'idée est que le délégué à la protection des données puisse faire des constats qui dérangent, ou donner des conseils qui n'arrangent pas l'employeur[41], sans craindre une mesure de représailles comme un licenciement.

En revanche, licencier un délégué parce qu'il exerce mal ses missions de délégué ou pour des motifs étrangers à sa fonction de délégué ne viole pas cette interdiction, pour autant que ces motifs soient dûment établis. Il sera donc prudent de solliciter de rapports d'activités et des avis écrits du délégué pour pouvoir objectiver les problèmes dans la qualité des prestations qui seraient rencontrés, le cas échéant[42]. Il n'y a pas d'atteinte à l'indépendance fonctionnelle du délégué dans ces cas-là. Au contraire, un délégué à la protection des données ne donnant pas satisfaction dans l'exercice de ses missions risque de mettre à mal l'objectif d'assurer un niveau élevé de protection des personnes physiques au sein de l'Union en ce qui concerne le traitement de leurs données à caractère personnel.

Fallait-il, du seul fait que le licenciement était, même partiellement, fondé sur la fonction de délégué, en déduire que la protection contre le licenciement visée à l'article 38, § 3, était ainsi violée ? En constatant, comme il l'a fait dans le cadre de la demande d'indemnité pour licenciement manifestement déraisonnable ou abusif, que le délégué à la protection des données ne menait pas ses missions à bien, le tribunal n'aurait-il pas donc dû conclure à une absence de violation de « l'interdiction de licenciement » prévue par l'article 38, § 3, du RGPD ? Nous le pensons.

Ce n'est toutefois pas la conclusion à laquelle le tribunal est arrivé et qui nous semblait pourtant trouver un écho certain dans la jurisprudence européenne, relayée, entre autres, par l'autorité belge de protection des données.

■ *François Schapira*
Avocat associé (Yelaw)

[40] Art. 10 de la loi du 20 décembre 2002 portant protection des conseillers en prévention, *M.B.*, 20 janvier 2003.

[41] K. Rosier, « Délégué à la protection des données : une nouvelle fonction, un métier en devenir », *op. cit.*, p. 157.

[42] *Ibid.*, p. 160.

Doctrine

De moeilijke kwalificatie van werknemers en andere vergelijkbare statuten onder de AVG[1]

Inleiding

Bij analyses omtrent de Algemene Verordening Gegevensbescherming (AVG) gaat vaak de meeste aandacht uit naar de rollen van de verwerkingsverantwoordelijke en de verwerker, de betrokkene of eventueel de functionaris voor gegevensbescherming. Juridisch gezien zijn dit de belangrijkste, maar zeker niet de enige, rollen in het kader van het personeel toepassingsgebied van de AVG.[2]

Vaak wordt er hierbij namelijk aan voorbijgegaan dat verwerkingsverantwoordelijken en verwerkers rechtspersonen zijn, die hun maatschappelijk doel realiseren via uitvoeringsagenten, d.w.z. diverse interne of externe medewerkers met uiteenlopende juridische statuten. Een rechtspersoon heeft als het ware 'handen' nodig om haar doel te bereiken. Het kan daarbij gaan om werknemers, vrijwilligers of freelance consultants of zelfs andere rechtspersonen.

Het is echter reeds lang aangenomen dat de rol van verwerkingsverantwoordelijke in principe wordt toegewezen aan de entiteit en niet de personen die onder het gezag van deze entiteit optreden.[3] Deze zogenaamde (interne en externe) medewerkers hebben tot voor kort

[1] De materie werd bijgehouden tot 4 september 2025.

[2] F. De Ridder en J. Vandendriessche, "Qualité des parties dans le cadre du RGPD : responsable (conjoint) du traitement ou sous-traitant – Quels critères, implications et opportunités stratégiques ?", *T. Verz.* 2024, afl. 28, 42-44.
Zie b.v. voor de klassieke benadering van het toepassingsgebied *ratione personae*: J. Doornaert, *La protection des données à caractère personnel et l'entreprise*, Wolters Kluwer, 2024, 30-34, rn. 200-230 ; C. De Terwangne, "Définitions clés et champ d'application du RGPD" in C. De Terwangne en K. Rosier, *Le règlement général sur la protection des données (RGPD/GDPR)*, Larcier, 2018, 67-69.

[3] B. Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, 2019,117, rn. 217.

maar weinig aandacht genoten van de wetgever, de rechtspraak en de rechtsleer. Een eenvoudige zoekopdracht in de wettekst van de AVG leert dat het begrip 'werknemer' slechts vier keer wordt gehanteerd. Tweemaal gebeurt dit inhoudelijk, d.w.z. dat de werknemer als voorwerp van een verwerking wordt vermeld.[4] Tweemaal worden werknemers vermeld als actor van een verwerkingsactiviteit.[5] Vrijwilligers en freelance consultants worden helemaal niet vermeld, althans niet als dusdanig.

De AVG vermeldt wel meermaals in verschillende bewoordingen de persoon die onder het (rechtstreeks) gezag van de verwerkingsverantwoordelijke of verwerker handelt of persoonsgegevens verwerkt.[6] Het mag allicht worden aangenomen dat dit tekstueel verschil (al dan niet rechtstreeks) geen juridische impact heeft.

De terminologische inconsistentie maakt een analyse er alvast niet gemakkelijker op.[7]

Daarnaast hanteert de AVG eveneens het begrip 'ontvanger' (artikel 4.9 AVG) en het begrip 'derde' (artikel 4.10 AVG). Hoe moeten personen die onder het gezag en onder de instructies van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken, worden beschouwd in het licht van deze begrippen?

Dit zal hieronder verder worden geanalyseerd. De kwalificatie van werknemers, vrijwilligers en freelance consultants is namelijk ontegensprekelijk belangrijk om enerzijds hun verplichtingen en anderzijds de verplichtingen van hun werkgever of opdrachtgever af te bakenen.

I. De kwalificatieproblematiek: wanneer is er sprake van een persoon die gerechtigd is persoonsgegevens te verwerken onder het rechtstreeks gezag en onder het toezicht van de verwerkingsverantwoordelijke of de verwerker?

Met het oog op de kwalificatie van werknemers, ambtenaren, vrijwilligers en freelance consultants, of zelfs andere statuten die in België of andere EU-lidstaten bestaan, is het belangrijk in het achterhoofd te houden dat volgens het Hof van Justitie bepalingen uit de AVG, die niet naar het recht van een lidstaat verwijzen, op een autonome en uniforme wijze dienen te worden geïnterpreteerd.[8]

Aangezien de AVG voor het begrip werknemer of personen die onder het (rechtstreeks) gezag van de verwerkingsverantwoordelijke of verwerker persoonsgegevens verwerken, niet verwijst naar het nationale recht, dienen deze begrippen dus autonoom te worden geïnterpreteerd.

Wanneer de AVG personen die onder het (rechtstreeks) gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken, vermeldt, dan dient dit begrip met andere woorden te worden geïnterpreteerd vanuit het perspectief van de gegevensverwerking. Het vereiste gezag is hierbij dan het recht van de verwerkingsverantwoordelijke (of de verwerker) om bindende instructies te verstrekken op het vlak van gegevensverwerking als inherent onderdeel van het statuut of de overeenkomst van de persoon aan wie de instructies worden gegeven. Dit gebeurt voor interne medewerkers veelal via een arbeidsovereenkomst. Naast de werknemers dient er nog een onderscheid te worden gemaakt tussen (i) ambtenaren (punt B), (ii) vrijwilligers (punt C) en (iii) zelfstandigen (punt D).

A. Werknemers

De arbeidsovereenkomst is de overeenkomst waarbij een werknemer zich verbindt, tegen loon, onder gezag, […] van een werkgever in hoofdzaak hoofdarbeid te verrichten.[9] Een kenmerkend gegeven van de arbeidsovereenkomst is de gezagsrelatie tussen de werkgever en de werknemer, die de werkgever toelaat instructies te geven aan de werknemer. Deze instructies kunnen vanzelfsprekend betrekking hebben op de verwerking van persoonsgegevens.

Er zijn diverse types arbeidsovereenkomsten. Een aantal arbeidsovereenkomsten worden geregeld door de Arbeidsovereenkomstenwet, terwijl andere arbeidsovereenkomsten worden geregeld door bijzondere wetten.[10]

Het Europees Comité voor Gegevensbescherming aanvaardt dat werknemers en personen met sterk vergelijkbare statuten vallen onder het begrip 'personen die persoonsgegevens verwerken onder het gezag en onder de instructies van de verwerkingsverantwoordelijke'.[11] Het statuut van de werknemer en andere vergelijkbare statuten (bv. jobstudenten, interim werk…) vallen bijgevolg onder het begrip 'personen die persoonsgegevens verwerken onder het gezag en onder het toezicht van de verwerkingsverantwoordelijke'.

B. Ambtenaren

Ambtenaren worden doorgaans aangeduid als personen die in dienst staan van een overheid.[12] Het personeel van de verschillende overheidsdiensten werkt doorgaans, en in zeer algemene termen uitgedrukt, in de context van een statuut of een overeenkomst.[13]

De verschillende statuten en overeenkomsten houden allen een element van tuchtregeling en/of gezag in, zodat

[4] Het betreft artikel 9.2.h AVG (de uitzondering voor verwerking van bijzondere categorieën van persoonsgegevens in de arbeidsrechtelijke context) en artikel 88 AVG (de zgn. openingsclausule voor verwerkingen in een HR-context).

[5] Het betreft artikel 39.1.a AVG (informatie en advies van de functionaris voor gegevensbescherming aan o.a. de werknemers) en artikel 47.1.a AVG (bindende bedrijfsvoorschriften, die bindend zijn t.a.v. o.a. werknemers).

[6] Het rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker: artikel 4.10 AVG. Het gezag van de verwerkingsverantwoordelijke of van de verwerker: artikel 29 AVG en artikel 32 AVG.

[7] Deze inconsistentie is reeds, weze het in mindere mate, aanwezig in Richtlijn 1995/46/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 (*Pb.* L 281, 23 november 1995, 31-50).

[8] HvJ 4 mei 2023, Österreichische Post, C-300/21, ECLI:EU:C:2023:370, nr. 29.

[9] Deze definitie is een veralgemeende vorm van de definitie van de arbeidsovereenkomst voor werklieden, bedienden, handelsvertegenwoordigers en dienstboden. Zie de artikelen 1, 2, 3, 4 en 5 van de wet van 3 juli 1978 betreffende de arbeidsovereenkomsten, *BS* 22 augustus 1978, zoals gewijzigd (hierna: Arbeidsovereenkomstenwet).

[10] B. Paternostre en M. Paternostre, "Wet betreffende de arbeidsovereenkomsten" in S. Goffin, V. Marcelle, L. Mesdom, J. Paternostre, M. Paternostre, J. Philippe, A. Vangansbeek en Z. Van Houdt, *Focus op Arbeidsovereenkomstenwet*, Kluwer, 2024, 2.

[11] European Data Protection Board, *Guidelines 07/2020 on the concept of controller and processor in the GDPR*, verbeterde versie 2.1 van 20 september 2022, 29, nr. 88.

[12] A. Beckers en W. Appels, "Gemeenschappelijke statutaire bepalingen" in A. Beckers en W. Appels, *Statutenzakboekje Overheidspersoneel*, Wolters Kluwer Belgium, 2024, 72.

[13] A. Beckers en W. Appels, "Gemeenschappelijke statutaire bepalingen" in A. Beckers en W. Appels, *Statutenzakboekje Overheidspersoneel*, Wolters Kluwer Belgium, 2024, 69-72.

het evident is ambtenaren eveneens te kwalificeren als personen die handelen onder het gezag en onder de instructies van de verwerkingsverantwoordelijke of verwerker.

C. Vrijwilligers

Het statuut van de vrijwilliger (in de ruime, feitelijke betekenis van het woord) of een persoon die aan liefdadigheid doet, is echter minder eenduidig te plaatsen onder de AVG omwille van de complexiteit van dit begrip in het Belgische recht, zelfs indien er zou worden uitgegaan van een autonome interpretatie.

In de eerste plaats dient er hierbij een onderscheid te worden gemaakt tussen (i) vrijwilligers die binnen het kader van de Vrijwilligerswet[14] vallen en (ii) vrijwilligers die erbuiten vallen (m.i.v. personen die zelf uit eigen beweging en buiten een structuur aan liefdadigheid of vrijwilligerswerk doen).

Volgens de Vrijwilligerswet is een vrijwilliger een natuurlijke persoon die vrijwilligerswerk verricht, nl. een activiteit die (a) onbezoldigd en onverplicht wordt verricht, (b) ten behoeve van één of meer personen, andere dan degene die de activiteit verricht, van een groep of organisatie of van de samenleving als geheel wordt verricht, (c) ingericht wordt door een organisatie anders dan het familie- of privéverband van degene die de activiteit verricht en (d) niet door dezelfde persoon en voor dezelfde organisatie wordt verricht in het kader van een arbeidsovereenkomst, een dienstencontract of een aanstelling als statutair personeelslid.[15]

Hoewel binnen dit kader een vrijwilliger niet mag worden beschouwd als een werknemer, lijkt het statuut voldoende vergelijkbaar qua regelmaat en organisatie om de vrijwilliger te beschouwen als een persoon die onder het gezag en de instructies van de verwerkingsverantwoordelijke of verwerker gemachtigd is persoonsgegevens te verwerken. Deze kwalificatie is niet onbelangrijk, aangezien de Vrijwilligerswet als voorwaarde stelt dat de organisatie niet binnen het familie- of privéverband mag vallen.[16] De uitsluiting van de verwerking van persoonsgegevens verricht door een natuurlijk persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit is hier door de wettelijke voorwaarde overduidelijk niet van toepassing (artikel 2.2.c AVG).

Voor de overige vrijwilligers, die niet binnen de definitie van de Vrijwilligerswet vallen, is een *ad hoc* analyse noodzakelijk. Deze vrijwilligers zullen doorgaans in twee categorieën kunnen worden ingedeeld.

Een eerste categorie betreft liefdadigheid en vrijwillig werk binnen de zuiver private sfeer. Het gaat bijvoorbeeld om een persoon die uit eigen beweging kleine giften doet aan behoeftigen of die een kleine klus verricht voor een kennis, vriend of familielid. Deze persoon valt overduidelijk onder de toepassing van de uitsluiting van zuiver persoonlijke of huishoudelijke activiteiten (artikel 2.2.c AVG), zodat de discussie rond de kwalificatie van deze persoon in het licht van de AVG irrelevant is. De AVG is immers niet van toepassing op deze verwerkingen van persoonsgegevens.

Een tweede categorie betreft vrijwilligers die onder een specifiek, ander wettelijk statuut vallen. Er kan bijvoorbeeld gedacht worden aan het sui generis-statuut van de vrijwilligers bij de brandweer en de civiele veiligheid. Deze vrijwilligers zullen in beginsel eveneens beschouwd worden als personen die persoonsgegevens verwerken onder het gezag en onder het toezicht van de verwerkingsverantwoordelijke.

D. Zelfstandigen (freelance consultants)

Ten slotte zijn er nog de zelfstandigen. Zelfstandige medewerkers, zij het onder de vorm van een eenmanszaak of via een managementvennootschap, kunnen niet worden beschouwd als personen die onder rechtstreeks gezag en onder de instructies van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Freelance consultants moeten bijgevolg als onderneming los worden gezien van de organisatie waarvoor zij persoonsgegevens verwerken. De hoedanigheid van afzonderlijke organisatie is overigens één van de basisvoorwaarden om als verwerker te worden aangeduid.[17] De kwalificatie van freelance consultants moet gebeuren zoals dit voor elke verwerkingsverantwoordelijke of verwerker gebeurt.[18] Doorgaans zal een freelance consultant als (sub)verwerker kwalificeren, maar andere kwalificaties (afzonderlijke verwerkingsverantwoordelijke of gezamenlijke verwerkingsverantwoordelijken) kunnen al naargelang de omstandigheden ook mogelijk zijn.

De typische gezagsrelatie die tussen werkgever en werknemer bestaat, ontbreekt bovendien steeds in deze relatie.

E. Samenvattende beschouwingen

Uit het bovenstaande kan er met andere woorden worden geconcludeerd dat werknemers (en vergelijkbare statuten), ambtenaren en vrijwilligers zullen worden beschouwd als personen die persoonsgegevens verwerken onder het gezag en onder de instructies van de verwerkingsverantwoordelijke of de verwerker. Zelfstandige medewerkers daarentegen kwalificeren als (afzonderlijke of gezamenlijke) verwerkingsverantwoordelijke of (meer waarschijnlijk) als (sub)verwerker, al naargelang de aard van de omstandigheden.

II. Het begrip 'ontvanger': zijn personen die onder het gezag van de verwerkingsverantwoordelijke of verwerker persoonsgegevens verwerken ontvangers?

Hoe verhoudt zich dit nu tot het begrip 'ontvanger'? Het begrip 'ontvanger' wordt gedefinieerd als "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. […]" (artikel 4.9 AVG).

Deze definitie bepaalt dat een partij gekwalificeerd wordt als ontvanger indien deze partij persoonsgegevens op enigerlei wijze verkrijgt of ontvangt. DE BOT merkt

[14] Wet van 3 juli 2005 betreffende de rechten van vrijwilligers, BS 29 augustus 2005.

[15] Artikel 3, eerste lid, 2° *juncto* artikel 3, eerste lid, 1° van de Vrijwilligerswet.

[16] Artikel 3, eerste lid, 1°, *littera* c van de Vrijwilligerswet.

[17] European Data Protection Board, *Guidelines 07/2020 on the concept of controller and processor in the GDPR*, verbeterde versie 2.1 van 20 september 2022, 25, nr. 76.

[18] Voor een meer diepgaande analyse: F. De Ridder en J. Vandendriessche, "Qualité des parties dans le cadre du RGPD: responsable (conjoint) du traitement ou sous-traitant – Quels critères, implications et opportunités stratégiques ?", *T. Verz.* 2024, afl. 28, 35-68.

hierbij overigens terecht op dat het woord 'verstrekken' ruim mag worden geïnterpreteerd.[19]

Uit deze definitie blijkt tevens dat de hoedanigheid van derde in de zin van artikel 4.10 AVG irrelevant is voor de kwalificatie als ontvanger. De vraag stelt zich dan ook of er in dit geval sprake kan zijn van interne en externe ontvangers.

A. De toepassing voorafgaand aan het arrest-Pankki[20]

Voor het arrest-Pankki werd in de rechtsleer unaniem een onderscheid gemaakt tussen interne ontvangers en externe ontvangers, d.w.z. partijen binnen de organisatie van de verwerkingsverantwoordelijke of verwerker aan wie gegevens worden verstrekt, dan wel partijen buiten de organisatie van de verwerkingsverantwoordelijke of verwerker aan wie gegevens worden verstrekt.[21] De ratio van dit onderscheid lag in (de perceptie van) het verschil in risico. Interne ontvangers werden namelijk steeds als inherent minder risicovol beschouwd.

Werknemers werden hierbij dan als interne ontvangers beschouwd, terwijl andere verwerkingsverantwoordelijken en verwerkers als externe ontvangers werden beschouwd.[22]

B. De toepassing sinds het arrest-Pankki

In het arrest-Pankki besliste het Hof van Justitie echter dat werknemers die onder het gezag en overeenkomstig de instructies van de verwerkingsverantwoordelijke persoonsgegevens verwerken geen ontvanger zijn in de zin van artikel 4.9 AVG.[23] Deze beslissing houdt dus een belangrijke wijziging in ten opzichte van de op dat ogenblik heersende rechtsleer.

De motivering voor deze beslissing is beperkt tot een verwijzing naar de Conclusie van Advocaat-Generaal Campos Sanchez-Bordona van 15 december 2022[24]. Advocaat-Generaal Campos Sanchez-Bordona is de mening toegedaan dat "[…] de werknemers van een rechtspersoon die, met gebruik van het computersysteem van die rechtspersoon, in opdracht van diens bestuursorganen de persoonsgegevens van een klant raadplegen" geen ontvangers zijn. Advocaat-Generaal Campos Sanchez-Bordona is van mening dat, "[w]anneer […] werknemers onder rechtstreeks gezag van de verwerkingsverantwoordelijke handelen, […] zij niet door dat enkele feit de hoedanigheid van 'ontvanger' van de gegevens [verkrijgen]".[25] Als onderbouwing voor dit standpunt verklaart Advocaat-Generaal Campos Sanchez-Bordona dat het Europees Comité voor Gegevensbescherming dezelfde mening is toegedaan[26]

Bij verdere analyse van de richtsnoeren van het Europees Comité voor Gegevensbescherming valt echter op dat het Europees Comité voor Gegevensbescherming niet uitdrukkelijk vermeldt of een werknemer al dan niet ontvanger is[27], maar wel expliciet stelt dat een werknemer geen derde is.[28] De richtsnoeren vermelden tevens als voorbeeld dat, wanneer persoonsgegevens aan een andere entiteit, zij het een verwerker of een derde, worden overgemaakt, deze andere entiteit een ontvanger is.[29] De vermelding dat een andere entiteit steeds een ontvanger is, laat evenwel niet toe om te besluiten dat een werknemer geen ontvanger zou zijn.

Gelet op het voorgaande is het dus niet mogelijk om de redenering van het Hof van Justitie en van Advocaat-Generaal Campos Sanchez-Bordona met zekerheid te doorgronden.

Het is mogelijk – echter niet met zekerheid vast te stellen – dat het Hof van Justitie aan de hand van deze uitspraak de gevolgen van het arrest-Österreichische Post[30] heeft willen afbakenen of temperen. In dat arrest besliste het Hof van Justitie dat de betrokkene bij een inzageverzoek het recht heeft, al naargelang de uitgedrukte keuze in het verzoek, op informatie over elke individuele ontvanger of de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt. Indien werknemers, zoals eerder door de rechtsleer aangenomen, interne ontvangers zouden zijn, dan zou een betrokkene via een inzageverzoek de individuele identiteit van elke werknemer betrokken bij de verwerking kunnen verkrijgen. Het zou bovendien niet mogelijk zijn om de schending van de privacy of de veiligheid van de werknemer in te roepen om deze informatie niet te verstrekken, aangezien de beperking van het inzagerecht op grond van artikel 15.4 AVG enkel van toepassing is op het recht om een kopie te verkrijgen.

[19] D. De Bot, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context*, Kluwer, 2020, 171, rn. 448. Zie voor een concrete toepassing van deze ruime interpretatie: Conclusie van Advocaat-Generaal Campos Sanchez-Bordona 15 december 2022, Pankki S, C-579/21, ECLI:EU:C:2022:1001, nr. 65.

[20] HvJ 22 juni 2023, Pankki S, C-579/21, ECLI:EU:C:2023:501.

[21] D. De Bot, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context*, Kluwer, 2020, 171, rn. 450; F. Dumortier, "La sécurité des traitements des données, les analyses d'impact et les violations de données" *in* C. De Terwangne en K. Rosier, *Le règlement général sur la protection des données (RGPD/GDPR)*, Larcier, 2018, 180 en 184 (in het bijzonder voetnoot 172); D. De Bot, *Verwerking van persoonsgegevens*, Kluwer, 2001, 56, rn. 74.

[22] De Commissie voor de bescherming van de persoonlijke levenssfeer (de rechtsvoorganger van de Gegevensbeschermingsautoriteit) omschreef bv. "individuen […] in directe relatie met de verantwoordelijke" als categorie van ontvangers: CBPL, Aanbeveling 06/2017 van 14 juni 2017 betreffende het register van de verwerkingsactiviteiten, 36. Het verwerkingsregister van de Franse toezichthoudende autoriteit vermeldt tot op heden werknemers als ontvangers (https://www.cnil.fr/sites/cnil/files/2024-06/registre_rgpd_de_la_cnil_0.pdf).

Op basis van het begrip 'derde' zou een verwerker eventueel ook als een interne ontvanger kunnen worden beschouwd. Een verwerker is immers geen derde in de zin van artikel 4.10 AVG. Deze redenering vindt echter geen bijval in de rechtsleer (cf. hoofdstuk 3.3).

[23] HvJ 22 juni 2023, Pankki S, C-579/21, ECLI:EU:C:2023:501, nr. 73.

[24] HvJ 22 juni 2023, Pankki S, C-579/21, ECLI:EU:C:2023:501, nr. 73, met verwijzing naar Conclusie van Advocaat-Generaal Campos Sanchez-Bordona 15 december 2022, Pankki S, C-579/21, ECLI:EU:C:2022:1001, nr. 63.

[25] Conclusie van Advocaat-Generaal Campos Sanchez-Bordona 15 december 2022, Pankki S, C-579/21, ECLI:EU:C:2022:1001, nr. 63.

[26] Conclusie van Advocaat-Generaal Campos Sanchez-Bordona 15 december 2022, Pankki S, C-579/21, ECLI:EU:C:2022:1001, voetnoot 24, met verwijzing naar Europees Comite Voor Gegevensbescherming, Richtsnoeren 07/2020 over de begrippen 'verwerkingsverantwoordelijke' en 'verwerker' in de AVG, 2 september 2020, nr. 83-90.

Volledigheidshalve moet opgemerkt worden dat de Advocaat-Generaal Campos Sanchez-Bordona voor zijn conclusie gebruik heeft gemaakt van een verouderde versie van de richtsnoeren. De richtsnoeren van 2 september 2020 (versie 1.0) waren op dat ogenblik reeds enige tijd vervangen door een nieuwe versie van 7 juli 2021 (versie 2.0, aangenomen na publieke consultatie), verder verbeterd op 20 september 2022 (versie 2.1). De finale versie bevat in de corresponderende randnummers (rns. 85-92) evenwel geen aanpassingen. In randnummer 19 van de finale versie wordt wel verduidelijkt dat werknemers in principe geen verwerkingsverantwoordelijken of verwerkers zijn. In deze bijdrage wordt verder steeds verwezen naar de finale versie van de richtsnoeren.

[27] European Data Protection Board, *Guidelines 07/2020 on the concept of controller and processor in the GDPR*, verbeterde versie 2.1 van 20 september 2022, 25, Rns. 90-92, en in het bijzonder rn. 92.

[28] European Data Protection Board, *Guidelines 07/2020 on the concept of controller and processor in the GDPR*, verbeterde versie 2.1 van 20 september 2022, 25, Rn. 88.

[29] European Data Protection Board, *Guidelines 07/2020 on the concept of controller and processor in the GDPR*, verbeterde versie 2.1 van 20 september 2022, 25, Rn. 92.

[30] HvJ 12 januari 2023, Österreichische Post, C-154/21, ECLI:EU:C:2023:3.

De Advocaat-Generaal Campos Sanchez-Bordona meent echter – onvermijdelijk vanuit zijn eigen conclusie dat een werknemer geen ontvanger is – dat er in de AVG geen aanknopingspunten zijn om te besluiten dat "elke betrokkene het recht heeft om kennis te nemen van de identiteit van de werknemers van de verwerkingsverantwoordelijke die toegang tot zijn gegevens hebben gehad, ook als dat in opdracht en onder leiding van die verwerkingsverantwoordelijke is gebeurd"[31] en dat het tegenovergestelde besluiten zelfs schadelijke gevolgen zou kunnen hebben voor de betrokken werknemers.[32]

In het arrest-Pankki neemt het Hof van Justitie hetzelfde standpunt over, namelijk dat werknemers in beginsel geen ontvanger zijn, en licht het de beperking van het recht om een kopie te verkrijgen verder toe in de context van een inzageverzoek met betrekking tot een logbestand waarin de namen staan van werknemers die bepaalde persoonsgegevens hebben geraadpleegd.[33] In deze toelichting vermeldt het Hof van Justitie hierbij heel nadrukkelijk de problematiek van de privacy van de werknemer.

Deze motivering maakt het aannemelijk dat het Hof van Justitie effectief de gevolgen van de eerdere rechtspraak heeft willen temperen.

Ongeacht deze redenen, kan men er evenwel niet omheen dat het Hof van Justitie uitdrukkelijk heeft beslist dat een werknemer in beginsel geen ontvanger is.[34]

Hoewel het Hof van Justitie enkel uitspraak doet over werknemers die onder het gezag en overeenkomstig de instructies van de verwerkingsverantwoordelijke persoonsgegevens verwerken, mag aangenomen worden dat de beslissing eveneens van toepassing is op (a) personen met een vergelijkbaar statuut die onder het gezag en overeenkomstig de instructies van de verwerkingsverantwoordelijke persoonsgegevens verwerken en op (b) die werknemers (en vergelijkbare statuten) die onder het rechtstreeks gezag van de verwerker gemachtigd zijn persoonsgegevens te verwerken. Deze personen worden immers ook vermeld in artikel 4.9 AVG en artikel 29 AVG. Maar wat dan met verwerkers die ook uitsluitend volgens de instructies van de verwerkingsverantwoordelijke persoonsgegevens mogen verwerken?

C. Enkele bedenkingen rond de kwalificatie van verwerkers

De rechtsleer beschouwt een verwerker doorgaans als een externe ontvanger.[35] In het licht van het arrest-Pankki kunnen hier minstens vraagtekens bij worden geplaatst. Het kan namelijk moeilijk worden ontkend dat bepaalde regels rond personen die onder het gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn persoonsgegevens te verwerken, en bepaalde regels met betrekking tot verwerkers sterke gelijkenissen vertonen.

Een verwerker is een entiteit die namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt, en dit in de context van een verwerkingsovereenkomst die verplicht moet opleggen dat de verwerker uitsluitend persoonsgegevens mag verwerken op schriftelijke[36] instructies van de verwerkingsverantwoordelijke (artikel 4.7 AVG *juncto* artikel 28.3.a AVG).

Artikel 29 AVG vermeldt dat "[d]e verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, […] deze uitsluitend [verwerkt] in opdracht van de verwerkingsverantwoordelijke […]".

De bewegingsruimte van de verwerker en van personen die gemachtigd zijn onder het gezag van de verwerkingsverantwoordelijke of de verwerker persoonsgegevens te verwerken, is dus zeer vergelijkbaar.

De verwerker en de personen die gemachtigd zijn om onder het gezag van de verwerkingsverantwoordelijke of de verwerker persoonsgegevens te verwerken, worden bovendien beiden uitgesloten uit het begrip 'derde' (artikel 4.10 AVG).

De aansprakelijkheid van de verwerkingsverantwoordelijke voor fouten van de verwerker of van personen die gemachtigd zijn persoonsgegevens te verwerken onder het gezag van de verwerkingsverantwoordelijke is eveneens vergelijkbaar, maar niet volledig identiek.

Wanneer een verwerker een inbreuk begaat, dan kan de verwerkingsverantwoordelijke zowel via de publieke handhaving (bv. administratieve geldboete[37]) als de private handhaving aangesproken worden (artikel 82 AVG, met dien verstande dat een aantal verdelingsregels van toepassing zijn). Hetzelfde geldt wanneer een persoon die handelt onder het gezag van de verwerkingsverantwoordelijke een inbreuk begaat. Een verwerkingsverantwoordelijke kan zich met andere woorden niet verschuilen achter het verzuim van personen die gemachtigd zijn onder diens gezag persoonsgegevens te verwerken.[38]

Binnen dit kader zijn er zeker argumenten te putten uit deze gelijkenis om te verklaren dat een verwerker evenmin een ontvanger is, althans voor zover de verwerker handelt binnen de contouren van zijn verwerkingsovereenkomst met de verwerkingsverantwoordelijke.

Dit vraagstuk zal echter vroeg of laat verder moeten worden uitgeklaard door het Hof van Justitie.

D. Praktische gevolgen van het arrest-Pankki en de kwalificatie van werknemers

Aangezien personen die onder het gezag van de verwerkingsverantwoordelijke of verwerker persoonsgegevens verwerken niet (langer) als ontvanger worden beschouwd, zijn er een aantal praktische gevolgen.

1. Herkwalificatieproblematiek: toch ontvanger en verwerkingsverantwoordelijke?

Het arrest-Pankki heeft verduidelijkt dat werknemers in beginsel geen ontvangers zijn, meer specifiek wanneer de werknemers persoonsgegevens verwerken onder het gezag van de verwerkingsverantwoordelijke en overeenkomstig diens instructies.

[31] Conclusie van Advocaat-Generaal Campos Sanchez-Bordona 15 december 2022, Pankki S, C-579/21, ECLI:EU:C:2022:1001, nr. 73.

[32] Conclusie van Advocaat-Generaal Campos Sanchez-Bordona 15 december 2022, Pankki S, C-579/21, ECLI:EU:C:2022:1001, nr. 75-79, en in het bijzonder nr. 76 en 77.

[33] HvJ 22 juni 2023, Pankki S, C-579/21, ECLI:EU:C:2023:501, nr. 75-83.

[34] HvJ 22 juni 2023, Pankki S, C-579/21, ECLI:EU:C:2023:501, nr. 73.

[35] D. De Bot, *De toepassing van de algemene verordening gegevensbescherming in de Belgische context*, Kluwer, 2020, 172, rn. 451

[36] De Nederlandstalige versie van dit artikel vermeldt 'schriftelijke instructies', terwijl andere taalversies 'gedocumenteerde instructies' vermelden. Het betreft allicht een vertaalfout.

[37] HvJ 5 december 2023, Nacionalinis, C-683/21, ECLI:EU:C:2023:949, nr. 84.

[38] HvJ 11 april 2024, Juris, C-741/21, ECLI:EU:C:2024:288, nr. 53.

Maar wat als de instructies van de werkgever niet worden nageleefd? Advocaat-Generaal Campos Sanchez-Bordona verduidelijkt binnen dit kader heel uitdrukkelijk wat de gevolgen zijn wanneer een werknemer zich niet houdt aan de gegeven instructies: "Nu kan zich het geval voordoen dat een werknemer de door de verwerkingsverantwoordelijke vastgestelde procedures niet volgt en zich op eigen initiatief onrechtmatig toegang verschaft tot gegevens van klanten of van andere werknemers. In die situatie zou de oneerlijke werknemer niet namens en ten behoeve van de verwerkingsverantwoordelijke handelen. In zoverre zou de oneerlijke werknemer kunnen worden aangemerkt als een 'ontvanger' aan wie (in figuurlijke zin) – al is het door eigen hand en daardoor onrechtmatig – persoonsgegevens van de betrokkene zijn 'verstrekt', of zelfs als (autonome) verwerkingsverantwoordelijke."[39]

Er moet dus steeds per geval worden nagegaan welke instructies de verwerkingsverantwoordelijke (of verwerker) heeft gegeven aan de werknemer en of de werknemer deze instructies heeft nageleefd.[40]

Indien blijkt dat een werknemer toch niet conform de instructies van de verwerkingsverantwoordelijke (of verwerker) heeft gehandeld, dan zal de werknemer in kwestie als ontvanger worden gekwalificeerd. Uit de bewoordingen van Advocaat-Generaal Campos Sanchez-Bordona kan hierbij worden afgeleid dat de herkwalificatie als ontvanger niet noodzakelijk ook de kwalificatie als verwerkingsverantwoordelijke inhoudt ("of zelfs als […] verwerkingsverantwoordelijke").[41] Voor deze kwalificatie is dus blijkbaar meer nodig dan het louter niet volgens de instructies handelen.

Er kan dus een onderscheid worden gemaakt tussen een eenvoudig verzuim in de uitvoering van een instructie en een overschrijding van de instructie door persoonsgegevens voor eigen doeleinden te gebruiken.

Het is dan ook de vraag wat er vereist is om tot een herkwalificatie van de werknemer als verwerkingsverantwoordelijke te komen. Mogelijk kan de interpretatie (naar analogie) van artikel 28.10 AVG (van toepassing op verwerkers) hier enige duiding bezorgen. Dit artikel stipuleert dat een verwerker die in strijd met de AVG de doeleinden en de middelen van een verwerking bepaalt, als een verwerkingsverantwoordelijke wordt beschouwd.

In het arrest-Nacionalinis geeft het Hof van een Justitie een ruime uitleg aan de toepassingsvoorwaarden van dit artikel 28.10 AVG. Meer specifiek bepaalt het Hof van Justitie hier dat in "situaties waarin de verwerker persoonsgegevens voor eigen doeleinden heeft verwerkt of waarin de verwerker deze gegevens heeft verwerkt op een wijze die onverenigbaar is met het kader of de wijze van verwerking zoals die door de verwerkingsverantwoordelijke was bepaald of op zodanige wijze dat redelijkerwijs niet kan worden aangenomen dat de verwerkingsverantwoordelijke daarmee zou hebben ingestemd", de verwerker overeenkomstig artikel 28.10 AVG moet worden beschouwd als verwerkingsverantwoordelijke.[42]

Toch mag niet te snel worden geoordeeld dat deze ruime interpretatie eveneens van toepassing zou kunnen zijn op werknemers. Er is immers geen equivalente bepaling voor personen die onder het gezag en volgens de instructies van de verwerkingsverantwoordelijke of verwerker persoonsgegevens verwerken. Het lijkt dan ook juister, althans tot het Hof van Justitie deze vraag verduidelijkt, om uitsluitend toepassing te maken van de criteria voor de bepaling van de verwerkingsverantwoordelijke overeenkomstig artikel 4.7 AVG, zijnde diegene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit lijkt ook de oplossing die wordt gehanteerd door het Europees Comité voor Gegevensbescherming.[43]

Wat er van deze discussie ook zij, het is in ieder geval vanuit dit opzicht sterk aanbevolen om de verwerkingsgerelateerde taken van werknemers afdoende gedetailleerd in een profiel- of taakomschrijving uit te werken. Dezelfde waarschuwing geldt overigens ook voor verwerkers. De aard van de verwerking moet overeenkomstig artikel 28 AVG steeds verplicht worden opgenomen in de verwerkingsovereenkomst (artikel 28.3, eerste lid AVG). Het is dan ook aanbevolen deze omschrijving meer gedetailleerd op te nemen.

2. Transparantieverplichtingen

De AVG bevat enkele transparantieverplichtingen met betrekking tot ontvangers.

De artikelen 13.1.e AVG (rechtstreekse inzameling) en 14.1.e AVG (onrechtstreekse inzameling) vereisen dat de betrokkene op de hoogte wordt gebracht van de ontvangers of categorieën van ontvangers. In tegenstelling tot hetgeen werd bepaald in artikel 15 AVG, ligt de beslissingsbevoegdheid om ontvangers individueel dan wel als categorie te vermelden, bij de verwerkingsverantwoordelijke. Ingevolge het arrest-Pankki is het dus niet langer juist om werknemers te vermelden als categorie van ontvangers.

Hetzelfde geldt voor de vermelding van ontvangers in het verwerkingsregister. Het verwerkingsregister dat een verwerkingsverantwoordelijke krachtens artikel 30.1 AVG dient op te stellen, dient "de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt […]" te vermelden (artikel 30.1.d AVG). In het kader van het arrest-Pankki is het dus evenmin correct om werknemers te vermelden als categorie van ontvangers in het verwerkingsregister.

3. Inzageverzoeken

Zoals hierboven reeds uitvoerig toegelicht, worden ingevolge het arrest-Pankki personen die onder het gezag van de verwerkingsverantwoordelijke of verwerker persoonsgegevens verwerken niet langer beschouwd als ontvangers.

Bij de behandeling van een verzoek tot inzage van een betrokkene op grond van artikel 15 AVG, dient de verwerkingsverantwoordelijke dan ook geen werknemers (meer) te vermelden in het antwoord op artikel 15.1.c AVG. Dit betreft zowel de categorieën van werknemers als individuele werknemers.

[39] Conclusie van Advocaat-Generaal Campos Sanchez-Bordona 15 december 2022, Pankki S, C-579/21, ECLI:EU:C:2022:1001, nr. 64-65.

[40] Het Hof van Justitie stelt vast dat dit in de verwijzingsbeslissing werd afgetoetst: HvJ 22 juni 2023, Pankki S, C-579/21, ECLI:EU:C:2023:501, nr. 72.

[41] Conclusie van Advocaat-Generaal Campos Sanchez-Bordona 15 december 2022, Pankki S, C-579/21, ECLI:EU:C:2022:1001, nr. 65.

[42] HvJ 5 december 2023, Nacionalinis, C-683/21, ECLI:EU:C:2023:949, nr. 85.

[43] European Data Protection Board, *Guidelines 07/2020 on the concept of controller and processor in the GDPR*, verbeterde versie 2.1 van 20 september 2022, 29, rn. 88

Wel is het zo dat bij uitoefening van het recht om een kopie te verkrijgen op grond van artikel 15.3 AVG nog steeds persoonsgegevens van werknemers kunnen zijn vermeld op de kopie. Op grond van artikel 15.4 AVG kunnen deze identificatiegegevens van werknemers echter desgevallend worden verwijderd, omdat de vermelding ervan afbreuk doet aan het recht op privacy van de werknemer. Het lijkt er zelfs op dat het arrest-Österreichische Post de toepassing van artikel 15.4 AVG ten aanzien van identificatiegegevens heeft vergemakkelijkt, aangezien het Hof van Justitie deze identificatiegegevens (van werknemers) nu uitdrukkelijk heeft uitgesloten uit de toepassing van artikel 15.1.c AVG (door te stellen dat werknemers geen ontvangers zijn zolang ze handelen binnen de instructies van hun werkgever).

4. Inbreuken in verband met persoonsgegevens

Hoewel het arrest-Pankki op het eerste gezicht geen impact heeft op de opvolging van inbreuken in verband met persoonsgegevens, mag er toch niet te snel worden besloten dat er helemaal geen impact is.

Artikel 33.3 AVG (melding van een inbreuk aan de toezichthoudende autoriteit) en artikel 34.2 AVG (melding van inbreuk aan de betrokkene) vergen niet uitdrukkelijk dat de toezichthoudende overheid en betrokkene(n) worden geïnformeerd over de identiteit van de werknemer die een inbreuk in verband met persoonsgegevens heeft gepleegd.

De herkwalificatieproblematiek (zoals toegelicht onder punt 3.4 (a)) zal echter tot gevolg hebben dat de werknemer die een inbreuk in verband met persoonsgegevens begaat, geherkwalificeerd wordt als een ontvanger en desgevallend zelfs ook als een verwerkingsverantwoordelijke in de plaats van een persoon die handelt onder het toezicht en gezag van de verwerkingsverantwoordelijke.

Deze herkwalificatie leidt tot een informatieplicht, die *de facto* wél een impact kan hebben op de communicatie van inbreuken in verband met persoonsgegevens.

Wanneer er zich een wijziging voordoet binnen de informatie die op grond van artikel 13 AVG of artikel 14 AVG moet worden meegedeeld aan de betrokkenen, dan dient de verwerkingsverantwoordelijke die informatie mee te delen aan deze betrokkenen. Door de herkwalificatie wordt de werknemer dan een ontvanger en zelfs potentieel een afzonderlijke verwerkingsverantwoordelijke. Indien de betrokkenen hiervan nog niet op de hoogte waren, dan dient deze nieuwe ontvanger of categorie van ontvangers sowieso te worden meegedeeld. Een verstandige betrokkene zal dan snel beseffen dat er zich met betrekking tot zijn of haar persoonsgegevens een inbreuk in verband met persoonsgegevens heeft voorgedaan. De verwerkingsverantwoordelijke is bijgevolg *de facto* in zekere zin verplicht om de betrokkene op de hoogte te brengen van een inbreuk in verband met persoonsgegevens, ongeacht het risiconiveau.

De betrokkene kan vervolgens ook meer informatie verkrijgen dan voorzien in artikel 34.2 AVG. Op grond van artikel 15.1.c AVG kan de betrokkene via een inzageverzoek exacte informatie (identificatiegegevens) opvragen over de ontvanger en dus over de persoon die de inbreuk heeft gepleegd. Het is niet mogelijk om deze informatieverstrekking te weigeren, aangezien de beperking voorzien in artikel 15.4 AVG enkel betrekking heeft op het recht om een kopie te verkrijgen.

5. Publieke handhaving

Toezichthoudende autoriteiten hebben op grond van artikel 58 AVG een resem bevoegdheden, die evenwel uitsluitend gericht zijn op de verwerkingsverantwoordelijken en verwerkers. Dit aspect van de publieke handhaving richt zich bijgevolg in beginsel niet op de werknemer.

De herkwalificatie van een werknemer kan echter de publieke handhaving ook richten op de werknemer, indien deze werknemer door herkwalificatie de hoedanigheid van verwerkingsverantwoordelijke verwerft. Hierdoor ontstaat er in zeker zin een versplintering van de publieke handhaving. De toezichthouder zal in dit geval immers moeten bepalen wie welke inbreuk heeft gepleegd.

De werknemer, die wordt geherkwalificeerd als afzonderlijke verwerkingsverantwoordelijke ingevolge een onrechtmatig handelen, zal allicht evenmin de overige verplichtingen onder de AVG naleven. Het lijkt namelijk weinig waarschijnlijk dat deze werknemer aan een dergelijke herkwalificatie heeft gedacht en de nodige stappen heeft gezet om bv. een verwerkingsregister op te stellen, een rechtsgrond te kiezen, een privacy statement op te stellen en, eventueel, een functionaris voor gegevensbescherming aan te stellen.

In deze situatie kan de werkgever, als oorspronkelijke (afzonderlijke) verwerkingsverantwoordelijke, desgevallend ook worden gesanctioneerd, indien deze werkgever is tekortgeschoten aan de eigen wettelijke (AVG) verplichtingen. Er kan hier bv. gedacht worden aan inbreuken op de verantwoordingsplicht (artikel 5 AVG, het gegevensbeschermingsbeleid (artikel 24 AVG), de beveiligingsplicht (artikel 32 AVG) en de meldplicht met betrekking tot inbreuken in verband met persoonsgegevens (artikel 33-34 AVG).

Deze versplintering zien we thans reeds duidelijk in de rechtspraak. In een beslissing van de Geschillenkamer van 1 april 2025 komt de Geschillenkamer tot het besluit dat een onrechtmatige consultatie, buiten elke instructie om, van een medisch dossier van een werknemer door een hiërarchisch overste, buiten de normale werkuren, ertoe leidt dat deze persoon als afzonderlijke verwerkingsverantwoordelijke kwalificeert. Dit leidt er vervolgens toe dat de Geschillenkamer de rechtmatigheid van deze consultatie niet verder onderzoekt, aangezien de hiërarchisch overste (als afzonderlijke verwerkingsverantwoordelijke) niet betrokken is in de hangende procedure. De Geschillenkamer zal vervolgens wel nagaan of de werkgever correct heeft gehandeld op het vlak van de inbreuk in verband met persoonsgegevens en de beveiliging.[44]

Het wordt overigens nog iets complexer wanneer er een verwerker tussenkomt in de verwerking. In het arrest-Nacionalinis bepaalde het Hof van Justitie dat "een entiteit [die als verwerkingsverantwoordelijke optreedt] niet alleen verantwoordelijk is voor elke verwerking van

[44] Geschillenkamer 1 april 2025, nr. 64/2025, in het bijzonder rn. 26-32 (kwalificatie), 35 (afzonderlijke handhaving), 40-48 (inbreuken in verband met persoonsgegevens) en 56-64 (veiligheidsmaatregelen), https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n0-64-2025.pdf.

persoonsgegevens die zij zelf uitvoert, maar ook voor de verwerking die namens haar wordt uitgevoerd".[45] Hieruit volgt dat een verwerkingsverantwoordelijke een administratieve sanctie (waaronder ook een administratieve geldboete) kan worden opgelegd "in een situatie waarin persoonsgegevens onrechtmatig zijn verwerkt, en niet die verantwoordelijke, maar een door hem ingeschakelde verwerker deze verwerking namens hem heeft uitgevoerd".[46]

Deze verantwoordelijkheid strekt zich echter niet uit "tot situaties waarin de verwerker persoonsgegevens voor eigen doeleinden heeft verwerkt of waarin de verwerker deze gegevens heeft verwerkt op een wijze die onverenigbaar is met het kader of de wijze van verwerking zoals die door de verwerkingsverantwoordelijke was bepaald of op zodanige wijze dat redelijkerwijs niet kan worden aangenomen dat de verwerkingsverantwoordelijke daarmee zou hebben ingestemd".[47]

Hoewel het Hof van Justitie zich in de zaak-Nacionalinis niet uitspreekt over personen die onder het gezag van de verwerkingsverantwoordelijke persoonsgegevens verwerken, mag worden aangenomen dat deze *ratio legis* naar analogie van toepassing is.

Binnen dit kader kan het niet genoeg worden onderstreept dat de omschrijving van de verwerkingsactiviteit van een verwerker of een werknemer cruciaal is om de verantwoordelijkheid voor onrechtmatig handelen van een verwerker of een werknemer zoveel als mogelijk af te wentelen op deze personen.

Ten slotte voorziet de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens[48] in specifieke strafbaarstellingen die wel van toepassing zijn op 'personen die handelen onder het (rechtstreeks) gezag van de verwerkingsverantwoordelijke of verwerker'. Zo viseert artikel 222 niet enkel de verwerkingsverantwoordelijke of de verwerker, maar ook hun aangestelden of gemachtigden. Artikel 223 viseert nadrukkelijk de persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of verwerker. Vergelijkbare bewoordingen zijn terug te vinden in de artikelen 226 en 227. Deze bepalingen zetten de verwerkingsverantwoordelijke en de verwerker (of hun vertegenwoordigers op grond van artikel 27 AVG) evenwel niet uit de wind, aangezien artikel 228 bepaalt dat zij burgerrechtelijk aansprakelijk zijn (en blijven) voor de betaling van de geldboeten waartoe hun aangestelden of gemachtigden worden veroordeeld.

6. Aansprakelijkheid

Hoe zit het dan verder met de aansprakelijkheid van werknemers? Artikel 82 AVG regelt het recht op schadevergoeding.[49] Het betreft een autonome aansprakelijkheidsvordering ten aanzien van de verwerkingsverantwoordelijke of de verwerker. Het is bijgevolg in beginsel niet mogelijk om een vordering op grond van artikel 82 AVG in te stellen tegen een werknemer.

Dit betekent echter niet dat geen enkele aansprakelijkheidsvordering mogelijk is. Het handelen van personen die gemachtigd zijn persoonsgegevens te verwerken onder het gezag en onder de instructies van de verwerkingsverantwoordelijke of de verwerker wordt geregeld door het statuut van deze personen onder de toepasselijke nationaalrechtelijke bepalingen. Voor de werknemer kan dan worden gedacht aan het arbeidsrecht en de arbeidsovereenkomst, met de sanctiemechanismen die daarin zijn voorzien. De betrokkene of een andere belanghebbende zou eveneens een klassieke aansprakelijkheidsvordering (dus buiten de toepassing van artikel 82 AVG) kunnen instellen.[50] De contouren van een dergelijke vordering worden eveneens bepaald door het nationale aansprakelijkheidsrecht.

Ingevolgde de herkwalificatieproblematiek zal een werknemer onder omstandigheden wel als verwerkingsverantwoordelijke kunnen worden aangesproken. In dat geval staat er wel een vordering op grond van artikel 82 AVG open. De vraag is dan uiteraard wel wat de financiële draagkracht van de persoon in kwestie is.

III. Het begrip 'derde': zijn personen die onder het gezag van de verwerkingsverantwoordelijke of verwerker persoonsgegevens verwerken derden?

Volledigheidshalve dient er in deze context nog te worden stilgestaan bij het begrip 'derde'. Volgens artikel 4.10 AVG is een derde "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken".

Uit deze definitie vloeit overduidelijk voort dat de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of verwerker gemachtigd zijn om persoonsgegevens te verwerken geen derden zijn in de zin van artikel 4.10 AVG.

Werknemers, ambtenaren en vrijwilligers zijn dus geen derden, althans voor zover zij conform de instructies van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn tussen te komen in de verwerking. Andere werknemers, ambtenaren en vrijwilligers zijn ten opzichte van de verwerking wel derde.

Aangezien het begrip 'derde' hoofdzakelijk wordt gebruik in de context van de rechtsgrond gerechtvaardigd belang[51], waar het mogelijk is zowel het gerechtvaardigd belang van de verwerkingsverantwoordelijke als van een derde in te roepen (artikel 6.1.f AVG), is de impact van deze kwalificatie eerder gering. Het komt er in essentie op neer dat de belangen van personen die gerechtigd zijn de persoonsgegevens te verwerken onder het gezag van de verwerkingsverantwoordelijke of de verwerker niet in aanmerking komen om als rechtsgrond te dienen, aangezien zij geen derden zijn. De belangen van andere

[45] HvJ 5 december 2023, Nacionalinis, C-683/21, ECLI:EU:C:2023:949, nr. 36 en nr. 84.

[46] HvJ 5 december 2023, Nacionalinis, C-683/21, ECLI:EU:C:2023:949, nr. 84.

[47] HvJ 5 december 2023, Nacionalinis, C-683/21, ECLI:EU:C:2023:949, nr. 85.

[48] Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018 (hierna: de Kaderwet).

[49] Voor een gedetailleerde analyse van het recht op schadevergoeding op grond van artikel 82 AVG: J. Vandendriessche en F. De Ridder, "Het vraagstuk van aansprakelijkheid onder de AVG: een analyse uit verschillende oogpunten", *T. Verz.* 2024, afl. 28, 215-253.

[50] N. Roland, "Quel est l'impact sur le RGPD du livre 6 du Code civil belge relatif à la responsabilité extracontractuelle ?", *DPO news* 2024, afl. 30, 15 en 16.

werknemers, vrijwilligers of ambtenaren komen dan weer wel in aanmerking, aangezien zij wel derden zijn.

IV. Wat zijn de verplichtingen van 'personen die handelen onder het (rechtstreekse) gezag van verwerkingsverantwoordelijke of verwerker' onder de AVG?

Ten slotte bevat de AVG zelf bijzonder weinig verplichtingen ten aanzien van personen die handelen onder het (rechtstreekse) gezag van verwerkingsverantwoordelijke of verwerker.

Artikel 29 AVG bepaalt dat "[d]e verwerker en eenieder die onder het gezag van de verwerkingsverantwoordelijke of van de verwerker handelt en toegang heeft tot persoonsgegevens, [...] deze uitsluitend [verwerkt] in opdracht van de verwerkingsverantwoordelijke, tenzij hij Unierechtelijk of lidstaatrechtelijk tot de verwerking gehouden is"[52].

Het valt hierbij overigens op dat de personen geviseerd door de wettelijke handelingsbeperking voorzien in artikel 29 AVG niet het voorwerp kunnen uitmaken van een administratieve sanctie. Artikel 58.2 AVG vermeldt corrigerende maatregelen voor inbreuken ten aanzien van de verwerkingsverantwoordelijke en de verwerker, terwijl de administratieve geldboete voorzien in artikel 83.4.a AVG voor schending van artikel 29 AVG enkel de verwerker viseert.

Conclusie

De arresten-Österreichische Post en -Pankki hebben een belangrijke impact op de manier waarop personen die onder het gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn persoonsgegevens te verwerken, worden gekwalificeerd.

De personen die onder het gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn persoonsgegevens te verwerken, worden niet langer als ontvanger in de zin van artikel 4.9 AVG beschouwd, tenzij zij handelen buiten de instructies van de verwerkingsverantwoordelijke of verwerker. Een eenvoudig verzuim is echter niet voldoende.

Deze herkwalificatie heeft, al dan niet *de facto*, een impact op o.a. de transparantieverplichtingen, de verplichtingen met betrekking tot inbreuken in verband met persoonsgegevens, de publieke handhaving en de aansprakelijkheidsregeling op grond van artikel 82 AVG. Deze impact kan soms als onwenselijk worden beschouwd.

De lege ferenda zou ervoor kunnen worden gepleit om de benadering toch om te gooien, maar dan met een uitgebreide toepassing van artikel 15.4 AVG. Indien personen die onder het gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken toch zouden worden beschouwd als ontvanger, dan zou de betrokkene opnieuw individuele of algemene informatie over de werknemers kunnen opvragen. De eventuele nadelige gevolgen van dit verzoek voor de betrokken werknemer kan worden opgevangen door de toepassing artikel 15.4 AVG uit te breiden naar artikel 15.1.c AVG. In dit geval zou de verwerkingsverantwoordelijke, rekening houdend met de rechten en vrijheden van de werknemer namelijk zelf kunnen beslissen om de exacte identiteit of enkel algemene informatie te verstrekken. Deze oplossing sluit overigens zeer sterk aan bij het standpunt van het Hof van Justitie rond de mededeling van identificatiegegevens uit logs bij verzoek om een kopie van persoonsgegevens.[53]

■ *Johan Vandendriessche*
Advocaat
Professor UGent

■ *Kirsten Van Gossum*
Advocaat

[51] Ook in deze zin: N. Broeckx, "GDPR-verantwoordelijkheid in de medische sector: een toepassing op medisch-wetenschappelijk onderzoek", *T. Gez.* 2019, afl. 2, 113, rn. 26.

[52] Een vergelijkbare verplichting is terug te vinden in de artikelen 54, 86, 119, 152 en 178 van de Kaderwet.

[53] HvJ 22 juni 2023, Pankki S, C-579/21, ECLI:EU:C:2023:501, nr. 81-83.

DPO pro mag

ANTHEMIS, Avenue des Arts, 6-9/510 à 1210 Bruxelles
Tél. 010/42.02.90 - www.anthemis.be
Éditeurs responsables / Verantwoordelijke uitgevers :
Marc-Olivier Lifrange et Elisabeth Courtens
Secrétariat de rédaction / Redactiesecretariaat :
Justine Minot
justine.minot@anthemis.be
Maquette et mise en page / Opmaak :
Matthieu Lepoutre
 ISSN : 2796-0307

Le *dpo pro mag* est un trimestriel composé d'articles originaux et de tirés à part du *DPO news* / *dpo pro mag* is een kwartaalblad samengesteld uit originele artikels en artikels overgenomen uit *DPO news*

Comité de rédaction / Redactiecomité :
Katia Bodard, Julie Lodomez, Saba Parsa, Nathalie Ragheno, Patrick Soenen

4 numéros par an / 4 nummers per jaar

La revue est réservée aux membres de dpo pro / Het tijdschrift is alleen toegankelijk voor de leden van dpo pro.

Anthemis

dpo pro