



EUROPESE TOEZICHTHOUDER
VOOR GEGEVENSBESCHERMING



JAARVERSLAG

SAMENVATTING '22



Meer informatie over de Europese Toezichthouder voor gegevensbescherming (EDPS) is te vinden op onze website: edps.europa.eu.

Op de website kunt u zich tevens [inschrijven](#) voor onze nieuwsbrief.

Waterford, Ierland - Brussel, België: Trilateral Research Ltd, Vrije Universiteit Brussel, 2023

© Ontwerp en foto's: Trilateral Research Ltd, EDPS & Europese Unie

© Europese Unie, 2023

Overname met bronvermelding is toegestaan. Voor gebruik of reproductie van foto's of ander materiaal waarvan het auteursrecht niet bij de Europese Toezichthouder voor gegevensbescherming berust, moet rechtstreeks toestemming aan de rechthebbenden worden gevraagd.

PRINT ISBN 978-92-9242-804-4 doi: 10.2804/349403 QT-AB-23-001-NL-C

PDF ISBN 978-92-9242-723-8 ISSN 1831-0575 doi: 10.2804/45199 QT-AB-23-001-NL-N

VOORWOORD

Het is mij een genoegen om het jaarverslag van de EDPS voor 2022 aan u voor te stellen. Het afgelopen jaar stemt tot nadenken. Het is een bewogen jaar geweest: uitdagend en hoopvol, moeilijk maar toch bemoedigend, voor de hele wereld, maar ook voor de EDPS.

De inval van Rusland in Oekraïne heeft dit jaar een ongekennde reactie van de Europese Unie (EU) ontketend. Die heeft het afgelopen jaar bewezen dat zij oplossingen weet te vinden voor de hele EU, vooral te midden van externe dreigingen; oplossingen die niet alleen blijken geven van solidariteit, maar die ook onze kernwaarden en -beginselen uitdragen. Dat is dan ook de reden waarom de EDPS zich het afgelopen jaar heeft ingespannen om te laten zien dat wij het grondrecht op gegevensbescherming zullen hooghouden, zelfs tijdens crisismomenten waarin we snel en efficiënt maatregelen moeten treffen en moeten reageren. Onze inspanningen om Europese wetgevers te ondersteunen bij het wetgevingsproces en toezicht te houden op de ontwikkeling van Eurojust, het Agentschap van de Europese Unie voor justitiële samenwerking, zijn het bewijs dat we samen sterker staan.

Ondanks de gebeurtenissen die de hele wereld hebben geraakt, was dit jaar ook een jaar van ambities en ontwikkeling – een moment om na te denken over een toekomst die de uitdagingen van vandaag de baas kan. In deze postpandemische context organiseerden



we op 16 en 17 juni in Brussel de conferentie met de titel “The future of data protection: effective enforcement in the digital world” (De toekomst van gegevensbescherming: effectieve handhaving in de digitale wereld). We mochten maar liefst 2000 deelnemers verwelkomen op deze conferentie, zowel offline als online, die samen één centraal doel deelden: het debat over de toekomst van de handhaving van de algemene verordening gegevensbescherming, vier jaar na de inwerkingtreding ervan, verder op gang brengen. Ik ben trots op dit evenement en op de zinvolle besprekingen die ontstonden tijdens onze tweedaagse conferentie. Ze hebben tot tastbare acties geleid in de gegevensbeschermingsgemeenschap. De toezeggingen die het Europees Comité voor gegevensbescherming heeft gedaan in de Verklaring van Wenen of de plannen van de Europese Commissie om een wetgeving voor te stellen die bepaalde procedurele aspecten van de grensoverschrijdende samenwerking tussen gegevensbeschermingsautoriteiten harmoniseert, zijn twee belangrijke voorbeelden van het effect dat onze conferentie heeft gehad. Ik ben benieuwd waar dit gesprek ons toe zal leiden en ik wil ook onze hele gemeenschap bedanken voor hun inzet bij deze besprekingen.

Als toezichthouder voor gegevensbescherming bij de instellingen, organen en instanties van de EU heeft de EDPS de bijzondere taak om exclusief toe te zien op overheidsinstanties. Die taak gaat gepaard met een gevoel van verantwoordelijkheid om bij te dragen aan de besprekingen over de rol van de staat binnen een democratische samenleving. Dit heeft ons er bijvoorbeeld toe aangezet om de voorlopige opmerkingen van de EDPS over moderne spyware te delen in een poging om een beter democratisch toezicht te houden op de handelingen van de rechtshandavingsinstanties en nationale veiligheidsdiensten.

In dit opzicht heeft de EDPS ook een bevel uitgevaardigd aan Europol om een groot aantal gegevens te wissen over personen van wie niet vaststaat dat zij betrokken zijn bij een criminele activiteit. Het antwoord van de wetgever op

deze kwestie was voor de EDPS aanleiding om het Hof van Justitie van de Europese Unie te verzoeken de met terugwerkende kracht toepasselijke bepalingen van de gewijzigde Europol-verordening nietig te verklaren, gezien onze stellige overtuiging dat de Europese Unie wereldwijde normen met betrekking tot de rechtsstaat en de democratische waarden kan - en moet - bepalen.

Daarom moeten binnen de EU zelf de hoogste normen worden nagestreefd. De komende jaren zullen we ons blijven inzetten om dit te verwezenlijken. Ik ben er zeker van dat volgend jaar nieuwe uitdagingen en lichtpuntjes zal hebben, maar ik sta klaar om die samen met ons dynamische en toegewijde EDPS-team het hoofd te bieden.



Wojciech Wiewiórowski
Europese Toezichthouder voor
gegevensbescherming

HOOFDSTUK 1

Over ons



1.1.

De EDPS

Wie zijn wij?

De [Europese Toezichthouder voor gegevensbescherming](#) (EDPS) is de onafhankelijke gegevensbeschermingsautoriteit van de Europese Unie die toezicht houdt op de verwerking van persoonsgegevens door de Europese instellingen, organen, en instanties ("EU-instellingen").

Wij adviseren EU-instellingen over nieuwe wetgevingsvoorstellen en initiatieven met betrekking tot de bescherming van persoonsgegevens.

Wij monitoren de impact van nieuwe technologieën op gegevensbescherming en werken samen met toezichthoudende autoriteiten om te waarborgen dat de EU-regels voor gegevensbescherming consequent worden gehandhaafd.

Onze missie

Gegevensbescherming is een grondrecht dat wordt gewaarborgd door het Europese recht. Wij staan een sterke gegevensbeschermingscultuur binnen de EU-instellingen voor.

Onze waarden en beginselen

Bij onze werkzaamheden laten wij ons leiden door de volgende vier waarden:

- **Onpartijdigheid:** wij houden ons aan het ons gegeven wetgevings- en beleidskader, zijn onafhankelijk en objectief, streven naar het juiste evenwicht tussen de belangen die in het geding zijn;
- **Integriteit:** wij nemen de hoogste gedragsnormen in acht en handelen te allen tijde onberispelijk;
- **Transparantie:** wij leggen uit wat we doen en waarom we dat doen, in duidelijke taal die voor iedereen begrijpelijk is;
- **Pragmatisme:** de behoeften van belanghebbende partijen begrijpen en oplossingen vinden die in de praktijk werken.

Wat we doen

Dit zijn onze vier belangrijkste werkgebieden.

- **Toezicht en handhaving:** wij monitoren de verwerking van persoonsgegevens door EU-instellingen om te waarborgen dat zij de regels voor gegevensbescherming naleven;
- **Beleid en raadpleging:** wij adviseren de Europese Commissie, het Europees Parlement en de Raad over wetgevingsvoorstellen en -initiatieven die verband houden met gegevensbescherming;
- **Technologie en privacy:** wij monitoren en beoordelen technologische ontwikkelingen die gevolgen hebben voor de bescherming van persoonsgegevens. Wij zien erop toe dat de systemen voor de verwerking van persoonsgegevens door de EU-instellingen passende waarborgen bieden om de naleving van de regels voor gegevensbescherming te garanderen. We zijn bezig met de digitale transformatie van de EDPS.
- **Samenwerking:** wij werken samen met toezichthoudende autoriteiten om consistente gegevensbescherming in de hele EU te bevorderen. Ons voornaamste platform voor samenwerking met gegevensbeschermingsautoriteiten is het [Europees Comité voor gegevensbescherming](#), waaraan we een secretariaat ter beschikking stellen en waarmee we een [memorandum van overeenstemming](#) hebben uitgewerkt waarin de voorwaarden voor onze samenwerking zijn vastgelegd.

Onze bevoegdheden

De bevoegdheden die wij als gegevensbeschermingsautoriteit van de EU-instellingen hebben, zijn vastgelegd in [Verordening \(EU\) 2018/1725](#) (hierna "EUVG" genoemd).

Op grond van deze verordening kunnen we bijvoorbeeld een waarschuwing doen uitgaan naar de EU-instelling die persoonsgegevens op onrechtmatige of oneerlijke wijze verwerkt; de EU-instellingen gelasten het verzoek tot uitoefening van de rechten van een betrokkene in te willigen; een tijdelijk

of definitief verbod op een bepaalde gegevensverwerkingshandeling opleggen; EU-instellingen een administratieve geldboete opleggen; of een zaak voorleggen aan het Hof van Justitie van de Europese Unie.

We hebben ook specifieke bevoegdheden om toe te zien op de manier waarop de volgende organen en instanties persoonsgegevens verwerken: Europol, het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving, op grond van Verordening (EU) 2016/794; Eurojust, het Agentschap van de Europese Unie voor justitiële samenwerking in strafzaken, op grond van Verordening (EU) 2018/1727, het EOM, het Europees Openbaar Ministerie, op grond van Verordening (EU) 2017/1939 en Frontex, het Europees Grens- en kustwachtagentschap.

Raadpleeg voor meer informatie over de EDPS de [pagina met veel gestelde vragen](#) op de website van de EDPS.

Raadpleeg voor meer informatie over gegevensbescherming in het algemeen de [pagina met de woordenlijst](#) op de website van de EDPS.

1.2.

EDPS-strategie 2020-2024

In een online tijdperk, waarin gegevens zich over grenzen bewegen, zal het recht op gegevensbescherming ten behoeve van mensen in de EU en daarbuiten worden versterkt door solidariteit binnen Europa en op internationaal niveau.

De [EDPS-strategie voor 2020-2024](#) is gericht op drie pijlers: **vooruitziendheid**, **actie** en **solidariteit** om een veiligere, eerlijkere en duurzamere digitale toekomst tot stand te brengen.

- **Vooruitziendheid:** wij streven ernaar om als omzichtige instelling toekomstgericht te kijken naar trends op het gebied van gegevensbescherming en de juridische, maatschappelijke en technologische context.
- **Actie:** wij ontwikkelen proactief hulpmiddelen voor Europese instellingen, organen en instanties waarmee ze wereldwijd toonaangevend kunnen zijn op het gebied van gegevensbescherming. Wij bevorderen samenhang in de activiteiten van handhavingsinstanties in de EU, waarbij meer nadruk ligt op ware Europese solidariteit, gezamenlijk gedeelde lasten en een gemeenschappelijke aanpak.
- **Solidariteit:** wij zijn ervan overtuigd dat rechtvaardigheid alleen mogelijk als ieders privacy in alle EU-beleid wordt gewaarborgd, en dat duurzaamheid bepalend moet zijn voor gegevensverwerking in het openbare belang.

HOOFDSTUK 2

Een blik op de toekomst: onze doelstellingen voor 2023 en daarna



Tussentijdse evaluatie van de strategie - “Vorm geven aan een veiligere digitale toekomst”

De [EDPS-strategie voor 2020-2024 “Vorm geven aan een veiligere digitale toekomst”](#) was een antwoord op de grote veranderingen in de wereld. De strategie werd begin 2020 uitgewerkt en omvat drie strategische pijlers voor de EDPS: **voortuitziendheid, actie en solidariteit**. Maar zelfs onze meest voortuitziende experts hadden de paradigmaverschuiving die zou volgen niet kunnen voorspellen. De COVID-19-pandemie, de oorlog in Oekraïne en de wereldwijde economische crisis zorgden allemaal voor het uitdagende klimaat waarmee we werden geconfronteerd nadat we onze 2020-strategie hadden vastgelegd.

Daarom hebben we in 2022 besloten om een tussentijdse evaluatie van onze strategie voor 2020-2024 uit te voeren. In eerste instantie wilden we met deze tussentijdse evaluatie nagaan welke vooruitgang al werd geboekt bij de doelstellingen die in de strategie zijn vastgelegd. Het was ook meteen het uitgelezen moment om te kijken of er een verschuiving van de focus nodig was in het licht van de veranderende wereldwijde context. In het volgende hoofdstuk van het jaarverslag worden de resultaten van de tussentijdse evaluatie voorgesteld, gevolgd door een uiteenzetting van de herziene visie en prioriteiten van de EDPS voor de rest van de strategie.

Procedure van de tussentijdse evaluatie

Er werd een ‘bottom-up’-aanpak gehanteerd voor de tussentijdse evaluatie. Dat betekent dat de strategie van binnenuit werd geëvalueerd. Die beslissing werd genomen om te putten uit de nieuwe perspectieven van de EDPS-medewerkers, rekening houdend met de institutionele groei die sinds

2020 heeft plaatsgevonden. Aan de hand van deze aanpak konden we de interne interdisciplinaire kennis en ervaring van het EDPS-personeel inzetten om de belangrijkste aandachtspunten voor ons werk in de komende jaren te bepalen.

De tussentijdse evaluatie verliep in twee fasen. De eerste fase bestond uit een analyse van de tekortkomingen. Eerst werden de doelstellingen in kaart gebracht door alle EDPS-medewerkers. Deze oefening kwam er officieel na een bespreking tussen de toezichthouder en de EDPS-medewerkers, waarin de toezichthouder de geplande procedure voorstelde om een open debat met het personeel op gang te brengen. Op basis van de waardevolle input van het personeel werden de doelstellingen in kaart gebracht. In deze oefening werden de 57 doelstellingen van de strategie van de EDPS voor 2020-2024 opgesomd. Voor elk van die doelstellingen gingen de EDPS-medewerkers na of en in welke mate ze werden behaald. Na deze voorlopige evaluatie werd een analyse van de tekortkomingen uitgevoerd om te kijken hoever we staan bij onze doelstellingen.

De resultaten van die oefening toonden aan dat er aanzienlijke vooruitgang is geboekt bij de implementatie en verwezenlijking van de doelstellingen uit de strategie. Uit de analyse is gebleken dat van de 57 doelstellingen die in de strategie worden vastgesteld tot nu toe 15 doelstellingen zijn behaald, nog 40 doelstellingen lopende zijn en dat slechts 2 doelstellingen zich in een beginfase bevinden.

De positieve resultaten van de analyse vormden de basis voor de tweede fase van de tussentijdse evaluatie. In deze tweede raadplegingsfase werden de EDPS-medewerkers geraadpleegd over de toekomst van de EDPS. Ze kregen de vraag of de nieuwe realiteit van onze context een verschuiving van de prioriteiten voor de rest van de strategie kan rechtvaardigen en op welke manier. Er werd specifiek bepaald op welke aandachtsgebieden de EDPS zich meer zou willen concentreren voor de rest van de strategie.

Resultaten van de tussentijdse evaluatie: van het vorm geven aan een veiligere digitale toekomst naar het verdedigen van die veiligere digitale toekomst

Uit de raadplegingsfase zijn verschillende institutionele prioriteiten naar voren gekomen, die voor ons cruciaal zijn en waaraan wij extra aandacht en middelen zullen besteden voor de rest van de strategie voor 2020-2024.

Prioriteit 1: effectieve handhaving van de gegevensbescherming in een nieuw regelgevingslandschap

Er zijn tal van wetgevingsinitiatieven op digitaal gebied aangenomen, en dus staat de EDPS, samen met de gemeenschap van gegevensbeschermingsautoriteiten, voor een aanzienlijk complexer regelgevingslandschap. Dit nieuwe regelgevingslandschap, met wetgeving zoals de datagovernanceverordening (DGA), de digitalemarktenverordening (DMA) en de digitaledienstenverordening (DSA) enerzijds en de voorgestelde wet op de artificiële intelligentie en

dataverordening anderzijds, heeft ertoe geleid dat de wetgever nieuwe regelgevende functies en regelgevende instanties voor ogen heeft.

Hoewel deze wetten en verordeningen in principe geen afbreuk doen aan de AVG (of de EUVG) of die wijzigen, verwijzen verschillende bepalingen in deze nieuwe of toekomstige regelgeving uitdrukkelijk naar definities, concepten en verplichtingen uit de AVG. En hoewel de verwerking van persoonsgegevens centraal staat bij de activiteiten die door elke wet of verordening worden geregeld, worden de gegevensbeschermingsautoriteiten niet als de belangrijkste bevoegde autoriteiten aangewezen. De handhaving wordt geheel of in zeer grote mate toevertrouwd aan autoriteiten wiens missie hoofdzakelijk betrekking heeft op andere beleidsdoelstellingen dan gegevensbescherming of privacy. Daarom is er een coherente aanpak nodig voor de regelgevingsactiviteiten in de digitale wereld. We zullen ons dan ook inzetten om onze rol ten aanzien van deze autoriteiten te conceptualiseren en om de verwachtingen van deze autoriteiten ten aanzien van de EDPS in kaart te brengen.

We staan bekend om onze uitgebreide ervaring met het waarborgen van een coherente aanpak in het digitale ecosysteem. Daarom zullen wij de leiding nemen over en actief meewerken aan de activiteiten van de relevante coördinatieorganen waarin de wet voorziet, zoals de groep op hoog niveau van de DMA en andere relevante coördinatieorganen waarin de wet voorziet, als zijnde de EDPS en lid van het Europees Comité voor gegevensbescherming.

We zullen ook actief inzetten op een sterke samenwerking met de betrokken instanties wanneer de wet niet in een specifieke coördinerende instantie voorziet, maar de handhaving wel vraagt om een nauwe dialoog met de autoriteiten die belast zijn met de toepassing van de bepalingen met betrekking tot privacy en gegevensbescherming.

Daarnaast zullen we ervoor zorgen dat de beginselen en regels voor gegevensbescherming niet worden ondermijnd door de toepassing en handhaving van de nieuwe wetgeving. De EDPS zal daarom onze adviserende functie blijven uitoefenen om de mogelijke gevolgen van de praktische implementatie van nieuwe regelgevingskaders op te volgen en te benadrukken. Waar nodig zullen ook handhavingsmaatregelen worden overwogen.

Het is in deze context dat de EDPS als toezichthoudende autoriteit van de instellingen, organen en instanties van de EU ("EU-instellingen") mogelijk ook een rol moet spelen op het gebied van artificiële intelligentie. Zowel vanuit organisatorisch als methodologisch oogpunt worden er intensieve voorbereidingen getroffen om ervoor te zorgen dat we vanaf het begin klaar zijn om onze nieuwe taak te vervullen.

Het Digital Euro-project is ook voor ons van groot strategisch belang en vraagt om een nauwe samenwerking tussen experts op het vlak van beleid, wetgeving, technologie en toezicht. Het Digital Euro-project zal ongetwijfeld grote gevolgen hebben voor de privacy en gegevensbescherming, al zal veel afhangen van de ontwerpkeuzes die worden gemaakt. Ook andere voorstellen met betrekking tot de financiële sector zullen vragen om een nauwlettend toezicht, zoals het wetgevingsvoorstel voor een nieuw kader voor een open geldwezen, dat de uitwisseling van gegevens en toegang van derden moet mogelijk maken voor een breed scala aan financiële sectoren en producten. We zullen daarom met de grootste aandacht nadenken over de mogelijke wisselwerking met de datagovernanceverordening en de dataverordening.

De [EDPS-conferentie](#) *The future of data protection: Effective enforcement in the digital world*, die in juni plaatsvond, heeft in grote mate de broodnodige vooruitgang in het publieke debat over de handhaving van de algemene verordening gegevensbescherming (AVG) op gang gebracht. Een aantal acties die werden genomen tijdens die conferentie, met name de zogenaamde [Verklaring van Wenen door het Europees Comité voor gegevensbescherming \(EDPB\)](#) en het aangekondigde voorstel van de Europese Commissie voor een verordening voor de harmonisering van bepaalde aspecten van nationale procedureregels, tonen aan dat de inspanningen voor mogelijke verbeteringen aan de werking van de AVG het debat de komende jaren zullen blijven domineren. Het succes van de EDPS-conferentie, met name op het gebied van algemeen belang en impact, toont dat er in dit debat een belangrijke rol is weggelegd voor de EDPS als onafhankelijke EU-instelling. De EDPS moet pleiten voor pan-Europese benaderingen die erop toezien dat het Handvest van de grondrechten van de Europese Unie ten volle wordt geëerbiedigd.

Prioriteit 2: de uitdaging van interoperabiliteit waarvoor een nieuwe manier van toezicht nodig is

Met de opkomst van de interoperabiliteit heeft de EDPS de belangrijke taak om het effectieve toezicht te waarborgen. De invoering van het interoperabiliteitskader van de EU, dat een nieuwe aanpak hanteert voor het beheer van gegevens voor grens- en veiligheidsdiensten, vraagt om een nieuwe methode voor het toezicht op grootschalige IT-systemen. Door de interoperabiliteitswijzigingen die het kader van de EU voorstelt, zullen tal van grootschalige IT-systemen worden gekoppeld aan de databanken van Europol en Interpol. Zo ontstaat een ecosysteem van gegevensstromen dat nog meer risico's met zich meebrengt voor betrokkenen als gevolg van de werking van de onderliggende systemen.

We hebben verschillende uitdagingen vastgesteld die we moeten aanpakken. De complexiteit van de algemene architectuur en de versplintering van de gegevensbeschermingsregels vragen om een bijgesteld toezicht dat zich richt op gegevensstromen in plaats van de afzonderlijke monitoring van de gegevensverwerking in verschillende systemen. Gezien de bijkomende gegevensverwerkingsactiviteiten die aanvankelijk niet zijn voorzien in het rechtsinstrument dat de opzet van elk van de onderliggende grootschalige IT-systemen regelt, is er een grondig onderzoek naar het doelbindingsbeginsel nodig. Bovendien worden er mogelijk beslissingen genomen die een aanzienlijke impact hebben op de gegevensbescherming bij comitologieprocedures en de overdracht van verantwoordelijkheden aan het Europees agentschap voor het operationeel beheer van grootschalige IT-systemen in de ruimte van vrijheid, veiligheid en recht (eu-LISA). Wanneer er geen centraal kanaal is waarmee de rechten van betrokkenen gelijktijdig in alle systemen kunnen worden uitgeoefend, kan dit leiden tot een versplintering van deze rechten.

De EDPS zal zich daarom toespitsen op de volgende drie prioritaire gebieden, die de basis zullen vormen voor ons toezicht op het interoperabiliteitskader tot het einde van het mandaat:

(1) Rechten van betrokkenen - We willen het risico op versplintering van de rechten van betrokkenen als gevolg van de verscheidenheid aan interoperabele databanken met verschillende verwerkingsverantwoordelijken aanpakken. Daarom zullen we de mogelijkheid voor gecoördineerd

toezicht onderzoeken (inclusief gezamenlijke reflectie met gegevensbeschermingsautoriteiten over het stroomlijnen van procedures voor de rechten van betrokkenen). Daarnaast willen we een proactieve aanpak uitwerken voor de rechten van betrokkenen, in het bijzonder het recht op informatie.

(2) Auditstrategie - We zullen een strategie op maat uitwerken voor gegevensbeschermingsaudits in de grootschalige IT-systemen en de interoperabiliteitsonderdelen, afgestemd op het nieuwe ecosysteem. Dat betekent mogelijk dat er een verschuiving plaatsvindt van audits van afzonderlijke systemen naar audits van gegevensstromen. De strategie omvat een gezamenlijke aanpak voor de audits van de interoperabiliteit, waarbij rekening wordt gehouden met verdere auditverplichtingen ten aanzien van agentschappen van de EU (Europol, Frontex, Eurojust), teneinde de doelbinding te waarborgen en na te gaan of deze entiteiten toegang hebben tot gegevens en deze verwerken overeenkomstig hun respectieve mandaten. Deze gezamenlijke aanpak zal een juridisch en een technisch gedeelte omvatten. Aangezien de regelgeving voor grootschalige IT-systemen de EDPS bovendien uitdrukkelijk verzoekt om “audits te verrichten overeenkomstig internationale auditnormen”, zal een gemeenschappelijke interpretatie van deze vereiste aan de orde zijn.

(3) Algoritmische profilering - De uitwerking van algoritmische profilering is met name bedoeld om de EDPS een plaats te geven binnen het interoperabiliteitskader (ETIAS en VIS) voor de toepassing van dit instrument, en algemener, om meer bepaald te focussen op kwesties als discriminatie, betrouwbaarheid, evenredigheid en transparantie. Het toezicht op de algoritmische profilering is een complexe taak die nog maar in een beginfase staat. Hiervoor is een samenwerking nodig met andere agentschappen en organen op het gebied van mensenrechten en de bestrijding van discriminatie, en mogelijk met andere spelers uit de burgersamenleving en de academische wereld. Met dit toezicht kunnen we onze inbreng voor zowel het ETIAS (het Europees reisinformatie- en autorisatiesysteem) en de Sturingsraad van het Visuminformatiesysteem voor de grondrechten (VIS) ondersteunen. We kunnen op die manier eveneens passende monitoring- en toezichtinstrumenten ontwikkelen voor dit nieuwe toezichtsgebied.

Prioriteit 3: internationale samenwerking ter bevordering van wereldwijde gemeenschappelijke benaderingen voor de uitdagingen op het gebied van privacy en gegevensbescherming

Wij vinden een actieve internationale samenwerking van fundamenteel belang. Op die manier kunnen we een bredere gemeenschap, buiten Europa, betrekken en een gemeenschappelijk inzicht en gemeenschappelijke aanpak voor de uitdagingen op het gebied van gegevensbescherming en privacy bevorderen. We zijn van plan onze inspanningen op het gebied van internationale samenwerking verder op te voeren, aangezien tal van onderwerpen van groot strategisch belang in internationale fora worden besproken.

We zijn met name van plan de coördinatie van de acties en strategie van leden van het Europees Comité voor gegevensbescherming in internationale fora te bevorderen, om verder te blijven werken in het kader van de GPA (Global Privacy Assembly), de Raad van Europa en de rondetafelconferentie van de gegevensbeschermingsautoriteiten van de G7, en de OESO (Organisatie voor Economische

Samenwerking en Ontwikkeling) door te zorgen voor de actieve deelname en effectieve vertegenwoordiging van de standpunten van de Europese autoriteiten en het Europees Comité voor gegevensbescherming. We willen ook de samenwerking met internationale organisaties en met regionale netwerken voor gegevensbescherming verder opvoeren.

Prioriteit 4: opnieuw nadenken over de processen van de EDPS om de efficiëntie in een snel veranderende wereld te waarborgen

De EDPS-strategie voor 2020-2024 is uitgerold in een periode waarin we de ene crisis na de andere zagen. Van de COVID-19-pandemie en de Russische inval in Oekraïne tot de stijgende energie- en inflatiekosten: we hebben onze werkwijzen en processen moeten aanpassen om onze doelstellingen te blijven verwezenlijken. We mogen er dan wel in geslaagd zijn om in principe de verbintenissen die we zijn aangegaan in de strategie na te komen, toch blijkt uit een interne analyse dat bepaalde processen verder moeten worden bijgesteld om onze efficiëntie en normen op lange termijn te verbeteren, zowel als Europese overheidsinstantie en als gegevensbeschermingsautoriteit.

In dat laatste geval gaat het onder meer om verbintenissen zoals het opvolgen van meldingen over gegevensinbreuken, het afhandelen van klachten of de mogelijkheid om kritieke nalevingsgerelateerde onderwerpen proactief aan te pakken via onderzoeken of audits. Er zal verder worden nagedacht over nieuwe instrumenten waarmee de naleving online of op afstand kan worden geëvalueerd. Tegelijkertijd vormen personeels- en budgettaire beperkingen een belangrijke belemmering voor de uitvoering van de toezichtstaken van de EDPS.

In dezelfde geest brengt de oorlog in Oekraïne nieuwe afzonderlijke taken mee voor de EDPS. In 2021 heeft de Europese Commissie een wetgevingspakket voorgesteld tot wijziging van de Eurojust-verordening om de verwerking van bewijsmateriaal dat is verzameld met het oog op het onderzoek naar oorlogsmisdaden gepleegd door Rusland mogelijk te maken. In 2022 werd nog een wetswijziging aangenomen, waarin Eurojust werd aangewezen als Europese hub voor de bewaring, opslag en analyse van bewijsmateriaal over ernstige internationale misdrijven. We hebben een belangrijke rol toebedeeld gekregen bij het opzetten van de nieuwe databank voor bewijsmateriaal. In januari 2023 kondigde de Europese Commissie de oprichting aan van het Internationaal Centrum voor de Vervolging van de Misdaad van Agressie (ICPA) bij Eurojust. Al deze wetswijzigingen hebben al geleid of zullen leiden tot aanzienlijk meer taken voor ons. Gezien het politieke belang van de steun van de EU aan Oekraïne en de aanzienlijke werklast die daarmee verbonden is, zullen onze activiteiten op dit gebied als een van onze belangrijkste prioriteiten worden gezien.

Er is steeds meer interesse in de werkzaamheden van de EDPS. Dat blijkt onder meer uit het aantal aanvragen voor de inzage van documenten. Daarom verbinden we ons ook tot strengere normen op het gebied van transparantie, niet alleen in het kader van goed bestuur, maar ook als een belangrijke manier om ons werk toegankelijk te maken voor burgers. We verbinden ons er ook toe een hoog niveau van gegevensbescherming en aansprakelijkheid te blijven waarborgen en het goede voorbeeld te geven, niet alleen door de wettelijke vereisten in acht te nemen, maar ook door belangrijke instrumenten en diensten voor privacy en gegevensbescherming te onderzoeken en in gebruik te nemen. We zullen ons ook moeten aanpassen aan de nieuwe voorschriften op het gebied van cyberbeveiliging om binnen alle EU-instellingen een hoog gemeenschappelijk niveau van cyberbeveiliging te waarborgen.

HOOFDSTUK 3

Onze hoogtepunten van 2022



3.1.

Onze bevoegdheden gebruiken om burgers te beschermen

Als toezichthoudende autoriteit voor gegevensbescherming zijn we belast met het toezicht op de instellingen, organen en instanties van de EU ("EU-instellingen"). Het is aan ons om erop toe te zien dat die EU-instellingen voldoen aan de Europese wetgeving inzake gegevensbescherming zodat burgers en hun grondrechten op het gebied van privacy en gegevensbescherming worden gewaarborgd.

Daarom verstrekken we richtsnoeren aan EU-instellingen, doen we aanbevelingen, geven we opmerkingen en adviezen, voeren we audits uit, verstrekken we opleidingssessies en stellen we andere middelen ter beschikking zodat ze over de geschikte instrumenten beschikken om de gegevensbescherming te garanderen bij hun dagelijkse taken, beslissingen of maatregelen waarbij persoonsgegevens worden verwerkt.

3.1.1.

Toezicht op de ruimte van vrijheid, veiligheid en recht

Van alle thema's waar wij moesten ingrijpen, ging onze aandacht vooral naar het toezicht op de ruimte van vrijheid, veiligheid en recht (RVVR) binnen de EU, die beleidsgebieden omvat, gaande van het beheer van de buitengrenzen, justitiële samenwerking in burgerlijke en strafzaken, alsmede asiel, migratie en misdaadbestrijding. De RVVR heeft betrekking op Europese agentschappen, zoals [Europol](#) (het Europese agentschap voor de samenwerking op het gebied van rechtshandhaving), [Frontex](#) (het Europese agentschap voor de grens- en kustwacht), [het EOM](#) (het Europees Openbaar Ministerie) en

[Eurojust \(het Europese agentschap voor justitiële samenwerking in strafzaken\)](#). Daarom speelden wij een bijzonder belangrijke rol, gezien de gevoelige aard van de informatie die wordt verwerkt en de grote gevolgen die dit kan hebben bij een verkeerde behandeling.

3.1.2.

Doorgiften van persoonsgegevens naar landen buiten de EU/EER

De internationale doorgifte van persoonsgegevens naar landen buiten de EU of de Europese Economische Ruimte (EER) heeft in de loop der jaren steeds meer onze aandacht gevraagd, ook in 2022. Die verplichtte ons om aanzienlijke middelen vrij te maken zodat het beschermingsniveau voor de persoonsgegevens van burgers gevrijwaard bleef.

Om die reden hebben we een aantal initiatieven genomen, advies verstrekt en aanbevelingen gedaan over hoe EU-instellingen de vereisten van de EU-wetgeving inzake gegevensbescherming moeten nakomen bij het gebruik van diensten of het sluiten van contracten met entiteiten buiten de EU/EER.



Het gebruik van producten en diensten afkomstig van landen buiten de EU/EER

Onze initiatieven omvatten ook lopende onderzoeken naar het gebruik van producten en clouddiensten van entiteiten buiten de EU/EER door EU-instellingen, in het bijzonder het gebruik van Microsoft Office 365 door de Europese Commissie, de uitgifte van richtsnoeren en beleidslijnen, en het verstrekken van opleidingen aan EU-instellingen. Deze inspanningen moeten EU-instellingen bewuster maken van de risico's die verbonden zijn aan het gebruik van instrumenten of het uitvoeren van gegevensverwerkingsactiviteiten waarbij gegevens worden doorgegeven naar landen buiten de EU/EER. We streven er ook naar de EU-instellingen bewuster te maken van de contractuele bepalingen

en administratieve regelingen, alsook van andere maatregelen die moeten worden genomen om ervoor te zorgen dat de persoonsgegevens buiten de EU/EER op in wezen gelijkwaardige wijze worden beschermd.

Gezien onze werkzaamheden op dit gebied en de EDPS-bevoegdheden hebben we toestemming gegeven voor een aantal doorgiftes van persoonsgegevens naar landen buiten de EU/EER in die gevallen waarin de EU-instellingen konden aantonen dat er deugdelijke procedures worden gevolgd en maatregelen worden genomen om ervoor te zorgen dat bij deze doorgiftes de persoonsgegevens van burgers worden beschermd.

Om in dit opzicht het goede voorbeeld te geven, werken we ook aan het gebruik van alternatieve producten en diensten van entiteiten die binnen de EU/EER gevestigd zijn, en moedigen we EU-instellingen aan dit ook te overwegen.

3.1.3.

Audit van grootschalige IT-systemen



Een van onze belangrijkste taken bestaat erin te garanderen dat de persoonsgegevens en privacy in de context van grootschalige IT-systemen in de ruimte van vrijheid, veiligheid en recht worden beschermd. En in dat opzicht voeren we audits uit bij deze systemen om ervoor te zorgen dat ze voldoen aan de regelgeving inzake gegevensbescherming en privacy.

Bij de uitvoering van deze audits beoordelen we de technische en organisatorische maatregelen die de systeembeheerders hebben genomen om ervoor te zorgen dat de systemen ontworpen zijn volgens de beginselen van 'privacy door ontwerp'. We bevorderen ook beste praktijken door de bevindingen en aanbevelingen van audits te delen met andere gegevensbeschermingsautoriteiten in de EU en door een cultuur van uitmuntendheid in gegevensbescherming en privacy in de hele EU tot stand te brengen.

Aan de hand van onze auditactiviteiten willen we EU-instellingen en het grote publiek bewust maken van het belang van gegevensbescherming en privacy in grootschalige IT-systemen. Door deze cruciale rol te vervullen, helpen wij de persoonsgegevens van Europese burgers te beschermen en zorgen wij ervoor dat grootschalige IT-systemen de hoogste normen op het gebied van gegevensbescherming en privacy in acht nemen.

In oktober 2022 hebben we in de kantoren van eu-LISA (het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen in de ruimte van vrijheid, veiligheid en recht) in Straatsburg een audit uitgevoerd bij drie grootschalige IT-systemen:

Eurodac, de Europese databank voor vingerafdrukken van asielzoekers, die helpt bij de verwerking van asielaanvragen.

SIS II, dat de interne veiligheid en de uitwisseling van informatie over personen en voorwerpen tussen nationale politie, grenscontrole, douane, visum- en gerechtelijke autoriteiten ondersteunt.

VIS, dat de toepassing van het gemeenschappelijke visumbeleid van de EU ondersteunt en grenscontroles en consulaire samenwerking vergemakkelijkt.

Bij de audit werden de methodologie en praktijken doorgelicht die eu-LISA gebruikt om systemen te ontwikkelen en te testen en er tegelijkertijd voor te zorgen dat de beginselen van beveiliging en gegevensbescherming door ontwerp en door standaardinstellingen worden toegepast. Daarnaast hebben we de maatregelen met betrekking tot het beheer van de IT-beveiliging, beveiligingsincidenten en inbreuken in verband met persoonsgegevens doorgelicht, en controleerden we of de aanbevelingen van onze vorige audits werden toegepast.

3.2.

Onze onafhankelijkheid beschermen

Nieuwe Europol-verordening: EDPS zet gerechtelijke stappen bij het Hof van Justitie van de Europese Unie

Op 16 september 2022 hebben wij het Hof van Justitie van de Europese Unie (HJEU) verzocht twee bepalingen van de onlangs gewijzigde Europol-verordening, die op 28 juni 2022 in werking is getreden, nietig te verklaren ([zaak T-578/22 - EDPS / Parlement en Raad](#)). De twee bepalingen hebben gevolgen voor de verwerking van persoonsgegevens die in het verleden door Europol is uitgevoerd. Daarbij ondermijnen de bepalingen de rechtszekerheid voor de persoonsgegevens van betrokkenen ernstig en zijn ze een gevaar voor de onafhankelijkheid van de EDPS.

3.3.

Vorm geven aan een veiligere digitale toekomst

Zoals we al stelden in de EDPS-strategie voor 2020-2024 waarderen we initiatieven waarbij in Europa aangemaakte gegevens worden omgezet in informatie met toegevoegde waarde voor Europese bedrijven en personen, en worden verwerkt in overeenstemming met Europese waarden, om een veiligere digitale toekomst vorm te geven. In dat opzicht hebben we de EU-wetgever advies gegeven over een breed scala aan aangelegenheden, zoals gezondheid, artificiële intelligentie en initiatieven om criminaliteit te helpen bestrijden.

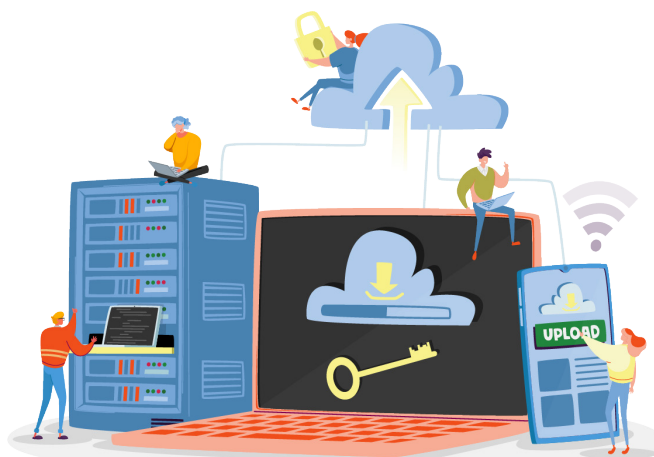
Normaal gezien verstrekken we advies aan de EU-wetgever over de voorgestelde wetgeving in de vorm van adviezen of formele opmerkingen. Onze **adviezen** worden uitgebracht als antwoord op verplichte verzoeken van de Europese Commissie, die wettelijk verplicht is om ons advies in te winnen voor elk wetgevingsvoorstel, alsook aanbevelingen en voorstellen aan de Raad in het kader van internationale overeenkomsten met een impact op de gegevensbescherming. Onze **formele opmerkingen** worden uitgebracht als antwoord op een verzoek van de Europese Commissie over ontwerpen van uitvoeringsnormen of gedelegeerde handelingen.

Wanneer een wetgevings- of ander relevant voorstel van bijzonder belang is voor de bescherming van persoonsgegevens, kan de Europese Commissie ook het Europees Comité voor gegevensbescherming (EDPB) raadplegen. In dergelijke gevallen werken de EDPS en het EDPB samen om een **gezamenlijk advies** uit te brengen.

De dataverordening van de EU

We hebben [samen met het EDPB een gezamenlijk advies uitgebracht over het voorstel voor de dataverordening](#), die tot doel heeft geharmoniseerde regels vast te stellen voor de toegang tot en het gebruik van gegevens die worden gegenereerd op basis van een breed scala van producten en diensten, waaronder verbonden objecten ('internet der dingen'), medische en gezondheidsapparatuur en virtuele assistenten.

In het advies wordt benadrukt dat gegevens moeten worden verwerkt volgens de Europese waarden als we vorm willen geven aan een veiligere digitale toekomst. Nu er nieuwe mogelijkheden voor het gebruik van gegevens worden gecreëerd, moet ervoor worden gezorgd dat het bestaande gegevensbeschermingskader volledig intact blijft. We hebben ook benadrukt dat de toegang tot gegevens door overheidsinstanties altijd naar behoren moet worden gedefinieerd en moet worden beperkt tot wat strikt noodzakelijk en evenredig is, wat niet het geval is in de ontwerpverordening.



De Europese ruimte voor gezondheidsgegevens

We hebben ook een [gezamenlijk advies uitgebracht over het voorstel voor de Europese ruimte voor gezondheidsgegevens](#) waarin we pleiten voor een solide bescherming van elektronische gezondheidsgegevens.

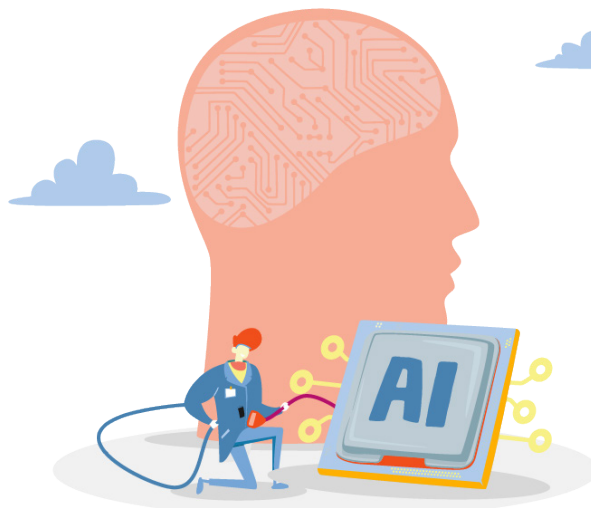
Het voorstel voor de Europese ruimte voor gezondheidsgegevens is het eerste van een reeks voorstellen voor domeinspecifieke gemeenschappelijke Europese gegevensruimtes. Het voorstel zal integraal deel uitmaken van de oprichting van een Europese gezondheidsunie die de EU in staat moet stellen om optimaal gebruik te maken van de mogelijkheden die samenhangen met het veilig en beveiligd uitwisselen, gebruiken en hergebruiken van gezondheidsgegevens.

Samen met het EDPB hebben we verschillende punten van zorg aangekaart, met name over het secundaire gebruik van elektronische gezondheidsgegevens.

Artificiële intelligentie

Zoals in onze EDPS-strategie voor 2020-2024 wordt benadrukt, wordt artificiële intelligentie (AI) steeds meer ingezet bij overheidsdiensten en in het strafrecht. Het is aan ons om ervoor te zorgen dat deze nieuwe technologie wordt gebruikt in overeenstemming met de EU-wetgeving inzake gegevensbescherming en dat de privacy van burgers wordt geëerbiedigd.

Naast de andere initiatieven die we hebben genomen of waaraan we hebben meegewerkt, hebben we een [advies uitgebracht over de aanbeveling voor een besluit van de Raad houdende machtiging tot het openen van onderhandelingen namens de Europese Unie over een verdrag van de Raad van Europa inzake artificiële intelligentie, mensenrechten, democratie en de rechtsstaat \("AI-verdrag"\)](#), dat we zien als een belangrijke stap om het eerste juridisch bindende nationale instrument inzake artificiële intelligentie te ontwikkelen op basis van de Europese normen en waarden inzake mensenrechten, democratie en de rechtsstaat, als aanvulling op de wet van de EU op de artificiële intelligentie. Niettemin benadrukten we de noodzaak om passende, krachtige en duidelijke waarborgen voor de gegevensbescherming op te nemen om personen die gevolgen ondervinden van het gebruik van AI-systemen te beschermen.



Misdaadbestrijding

We hebben een reeks adviezen uitgebracht over diverse voorstellen op het gebied van het strafrecht.

Een van onze adviezen die samen met het EDPB werd uitgebracht richtte zich bijvoorbeeld op een [voorgestelde verordening ter voorkoming en bestrijding van seksueel misbruik van kinderen](#). Wij hebben onze steun getoond voor de doelstellingen van het voorstel, maar zijn bezorgd dat het meer risico's kan inhouden voor burgers en bij uitbreiding voor de samenleving in het algemeen dan voor de criminelen die voor seksueel misbruik van kinderen worden vervolgd.

Een ander opmerkelijk voorbeeld van onze aanbevelingen en richtsnoeren betrof het thema van internationale samenwerking voor de misdaadbestrijding. We hebben met name een [advies](#) uitgebracht over twee voorstellen: het eerste om de EU-lidstaten te machtigen om het [tweede aanvullend protocol](#) bij het [Verdrag van Boedapest inzake cybercriminaliteit](#) te ondertekenen, en het tweede om de EU-lidstaten te machtigen hetzelfde protocol te bekrachtigen.

Misdrijven onderzoeken en vervolgen mag dan wel een gerechtvaardigd doel zijn waarbij de internationale samenwerking en de uitwisseling van gegevens een grote rol spelen, toch benadrukten we het belang aan duurzame overeenkomsten met de EU voor de uitwisseling van persoonsgegevens met landen buiten de EU met het oog op de rechtshandhaving. Deze overeenkomsten moeten volledig verenigbaar zijn met het recht van de EU, met inbegrip van de grondrechten op privacy en gegevensbescherming.

3.4.

De toekomst van gegevensbescherming: effectieve handhaving in de digitale wereld



In juni 2022 organiseerden we onze EDPS-conferentie, met de titel [“The Future of Data Protection: Effective Enforcement in the Digital World”](#), die meer dan 2000 deelnemers samenbracht, zowel in Brussel als online. Er waren meer dan honderd sprekers, drie hoofdsessies, zestien break-outsessies,

negen individuele toespraken rond een centraal thema en vijf nevenevenementen. Het tweedaagse evenement heeft cruciale gesprekken over de toekomst van gegevensbescherming op gang gebracht, met bijzondere aandacht voor de handhaving van de algemene verordening gegevensbescherming (AVG).

Onze langetermijnvisie voor de toekomst van gegevensbescherming is duidelijk: de handhaving moet op een pan-Europese manier worden benaderd om een echt en consequent hoog niveau van bescherming voor personen te kunnen waarborgen en de belofte van de AVG te kunnen nakomen.

3.5.

Monitoring van de technologie en vooruitziendheid

Een van de drie hoofdpijlers van de EDPS-strategie voor 2020-2024 is **vooruitziendheid**. We stellen namelijk alles in het werk om als omzichtige instelling toekomstgericht te kijken naar trends op het gebied van gegevensbescherming en de ontwikkeling van de juridische, maatschappelijke en technologische context.

Een van de manieren waarop we in de praktijk toekomstgericht te werk gaan is door in gesprek te gaan met experts, specialisten en gegevensbeschermingsautoriteiten. We trachten inzicht te krijgen in de technologieën, we analyseren de gevolgen ervan voor de gegevensbescherming en de privacy van burgers om zo kennis te delen en de ontwikkeling van deze nieuwe en opkomende technologieën op een privacyconforme manier te benaderen. **TechSonar** en **TechDispatch** zijn twee van onze initiatieven op dit gebied.

TechSonar is bedoeld om te anticiperen op nieuwe technologische trends. Het belangrijkste doel van dit initiatief is om de toekomstige ontwikkelingen in de technologische sector beter te begrijpen vanuit het oogpunt van gegevensbescherming. Op basis van onze gezamenlijke inspanningen, door trends in kaart te brengen, te brainstormen, te evalueren, te publiceren, te bepleiten en continu te monitoren, willen we een bijdrage leveren aan het grotere debat over toekomstgerichtheid binnen de EU-instellingen. Het tweede jaarlijkse [TechSonar-verslag](#), dat op 10 november 2022 werd gepubliceerd, gaat dieper in op vijf technologieën die we het komende jaar in de gaten moeten houden. Dat zijn de digitale valuta van de centrale bank, metaverse, synthetische gegevens, 'federated learning' en opsporingssystemen voor nepnieuws.



TechDispatch is bedoeld om opkomende technologische ontwikkelingen toe te lichten. De verslagen van TechDispatch, waarvoor we in 2021 een award van de Global Privacy Assembly in ontvangst mochten nemen, maken deel uit van de bredere EDPS-activiteiten rond [de monitoring van technologieën](#). Elke TechDispatch geeft feitelijke beschrijvingen van een nieuwe technologie, geeft een voorlopige beoordeling van de mogelijke gevolgen ervan voor de privacy en de gegevensbescherming, zoals we ze nu begrijpen, en verstrekt links naar andere artikelen voor meer informatie. Dit jaar richt TechDispatch, dat werd gepubliceerd in juli 2022, zich op Fediverse en gefedereerde socialemediaplatformen.



3.6.

Digitale innovatie

De bevordering van gegevensbeschermingsvriendelijke instrumenten die de grondrechten van burgers eerbiedigen en vooropstellen tijdens hun ontwikkeling en gebruik is één van de kerndoelstellingen van de EDPS-strategie voor 2020-2024. Om deze doelstellingen te behalen, zijn we op zoek gegaan (en dat blijven we ook doen) naar alternatieve instrumenten, met name communicatie- en samenwerkingstools, die voldoen aan de EU-wetgeving en -normen inzake gegevensbescherming. Door deze alternatieve instrumenten zelf te gebruiken, willen we EU-instellingen aanmoedigen om ons voorbeeld te volgen. Op die manier kunnen we collectief onze afhankelijkheid van monopolistische voorzieningen minimaliseren en zo schadelijke lock-in voorkomen.

We spelen een belangrijke rol bij het bevorderen van digitale innovatie door het goede voorbeeld te geven, bijvoorbeeld door open-sourcetoepassingen en -platformen te gebruiken die privacyvriendelijke alternatieven bieden voor bijvoorbeeld producten en diensten van grote techbedrijven. Onze inspanningen voor privacy strekken zich uit tot zowel sociale netwerken als samenwerkingstools, met initiatieven zoals EU Video, EU Voice en de proefprojecten van Nextcloud.

In februari 2022 lanceerden we de proeffase van twee socialemediaplatformen: [EU Voice](#), waarop we regelmatig berichten over onze activiteiten publiceren, en [EU Video](#), waarop we video's publiceren, als aanvullende alternatieve communicatiekanalen om met ons publiek te communiceren. Beide platforms maken deel uit van gedecentraliseerde, vrije en opensource-socialemedianetwerken die gebruikers verbinden in een privacygerichte omgeving, op basis van Mastodon- en PeerTube-software. Beide projecten leggen de nadruk op de bescherming van gegevens en de privacy van gebruikers, en zorgen ervoor dat EU-instellingen toegang hebben tot communicatietools die aansluiten bij de Europese waarden en beginselen, zonder hun persoonsgegevens in gevaar te brengen.



Naast sociale netwerken steunen we het gebruik van alternatieve samenwerkingstools die privacy vooropstellen. Het proefproject Nextcloud is een uitstekend voorbeeld van deze verbintenis. Nextcloud is een zelfgehost opensource-cloudplatform waarmee gebruikers veilig bestanden, agenda's en contacten kunnen opslaan, delen en daaraan samenwerken. Door privacybewuste tools zoals Nextcloud te promoten en te gebruiken, tonen we dat we een digitaal ecosysteem willen promoten waarin de beginselen inzake gegevensbescherming en privacy worden geëerbiedigd. Zo helpen we uiteindelijk bij de ontwikkeling van innovatieve en privacyvriendelijkere alternatieven.

Tijdens de EDPS-conferentie in juni 2022, met de titel [“The Future of Data Protection: Effective Enforcement in the Digital World”](#) hebben we ook een oplossing op maat voor videoconferenties ontwikkeld die volledig voldoet aan de vereisten voor de gegevensdoorgifte op grond van de AVG en de EUVG. Zo kunnen we het goede voorbeeld geven en het pad vrijmaken voor de naleving van de vereisten inzake gegevensbescherming. Als gegevensbeschermingsautoriteit die bevoegd is voor het toezicht op alle EU-instellingen was het belangrijk voor ons om aan te tonen dat het mogelijk is om de regelgeving na te leven in videoconferentietools en in het bijzonder om te voldoen aan de regels voor de gegevensdoorgifte bij de doorgifte van persoonsgegevens naar landen buiten de EU en de EER.

3.7.

Communicatie over gegevensbescherming



Als organisatie is het ons doel om op een transparante, duidelijke en interactieve manier uit te leggen wat we doen en waarom we dat doen, want het is belangrijk dat Europese burgers hun rechten in verband met gegevensbescherming kennen en weten hoe die kunnen worden beïnvloed.

Een steeds grotere aanwezigheid online

De EDPS heeft een gevestigde online aanwezigheid op verschillende socialemediakanalen, met name [Twitter](#) (29 100), [LinkedIn](#), waar we dit jaar meer dan 63 000 volgers hebben, [YouTube](#) (2750), [EU Voice](#) (5100) en [EU Video](#) (690), waardoor we ons wereldwijde publiek gemakkelijk en snel kunnen bereiken.

We creëren in grote lijnen content om aan de hand van campagnes zichtbaarder te worden en om de deelname van de EDPS aan evenementen live te tonen.

Gegevensbescherming dichterbij de burgers brengen

Gegevensbescherming kan soms heel complex zijn. Daarom stellen we alles in het werk om content over gegevensbescherming te creëren die zowel geschikt is voor experts als niet-experts. Zo brengen we onze werkzaamheden dichterbij de burger.

We stellen bijvoorbeeld [maandelijks nieuwsbrieven](#) op, geven korte, hapklare uitleg over onze nieuwste initiatieven en de impact die ze kunnen hebben op het publiek, we maken [factsheets](#) waarin we belangrijke concepten van gegevensbescherming toelichten, we voeren socialemediacampagnes uit en werken samen met andere EU-instellingen om mensen bewust te maken van gegevensbeschermingskwesties. Dit jaar gingen we een stap verder in deze richting en lanceerden we een nieuwe podcastserie, [Newsletter Digest](#), om een groter publiek te bereiken en hen te informeren over wat we doen om hun gegevens te beschermen.

Media en public relations

We hebben regelmatig contact met de media, vooral via onze persberichten over belangrijke initiatieven voor gegevensbescherming die in de hele EU een grote impact hebben. Dit jaar waren er tal van onderwerpen die heel wat aandacht kregen, gevolgd door aanvragen voor vervolggesprekken of interviews, zoals het toezicht op Europol en Frontex of onze EDPS-conferentie in juni.

En we werken op dezelfde manier aan onze relatie met het publiek, door vragen van burgers over ons werk en onze bevoegdheden als EU-instelling te beantwoorden en door studiebezoeken te organiseren in onze gebouwen.

Bijbenen na COVID-19

Nadat de COVID-19-beperkingen geleidelijk aan werden afgebouwd, konden we opnieuw evenementen organiseren, meer fysieke activiteiten laten plaatsvinden en deze evenementen toch afstemmen op de post-COVID-wereld. Onze evenementen en activiteiten werden ontworpen voor deelnemers online en offline. Tegelijkertijd konden we zo als organisatie onze impact op het milieu verminderen. Sindsdien zijn we erin geslaagd om twee grote hybride evenementen te organiseren: de conferentie "[The future of Data Protection. Effective enforcement in the digital world](#)" (De toekomst van gegevensbescherming: effectieve handhaving in de digitale wereld) in juni 2022, met 2000 offline en online deelnemers, en onze "[Supervision Conference: Data protection and criminal justice](#)" (conferentie rond toezicht: gegevensbescherming en strafrecht) in november 2022, met meer dan 200 online en offline deelnemers. Bij de meeste van onze evenementen hebben we ons beste beentje voorgezet om 'groener' te worden door te kiezen voor lokale catering, door voedselverspilling te vermijden en door ons merkmateriaal lokaal in te kopen, gemaakt van herbruikbare materialen.

Gezamenlijke communicatie

In 2022 hebben we samengewerkt met andere EU-instellingen aan gemeenschappelijke communicatieactiviteiten. In oktober sloegen we de handen in elkaar met ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging) en de Europese Commissie om een campagne te lanceren voor de [Europese maand van de cyberbeveiliging](#), ter gelegenheid van de 10de verjaardag. Daarnaast hebben we ideeën en ondersteuning aangereikt op het gebied van gegevensbescherming ten behoeve van de interinstitutionele onlinecommunicatiecommissie (IOCC). Voor de proefprojecten EU Voice en EU Video hebben we meer bepaald uitgebreid samengewerkt met de IOCC om redactionele richtsnoeren en serverbeleidslijnen te verstrekken en om hulp te bieden aan EU-instellingen die aan het project deelnemen.

3.8.

Een organisatie in verandering

Om onze doelstellingen te ondersteunen, met name de doelstellingen van onze EDPS-strategie voor 2020-2024, hebben we onze organisatie uitgebreid en andere veranderingen doorgevoerd om onze manier van werken beter te weerspiegelen.



We hebben de interne organisatie van de EDPS aangepast, een specifieke Juridische Dienst opgericht en de Governance en Internal Compliance Sector gecreëerd om de nodige expertise te verwerven om bepaalde taken te kunnen uitvoeren.

Onze doelstellingen verwezenlijken betekent ook dat we onze middelen zorgvuldig moeten inzetten. In dit opzicht werd er veel geïnvesteerd in de planning, uitvoering en controle van onze begroting.

Wij hebben ook de nodige voorbereidingen getroffen voor de opening van een EDPS-verbindingsbureau in Straatsburg, dat begin 2023 officieel zal worden ingehuldigd, ter versterking van de interinstitutionele en internationale samenwerking en om aanvullend advies te kunnen verstrekken op het gebied van gegevensbescherming.

Kernprestatie-indicatoren voor 2022

Wij gebruiken een aantal kernprestatie-indicatoren (KPI's) om onze prestaties af te zetten tegen de belangrijkste doelstellingen van de EDPS-strategie. Hierdoor kunnen wij onze activiteiten zo nodig aanpassen om meer zoden aan de dijk te zetten met onze activiteiten en onze middelen doeltreffender in te zetten.

Het onderstaande KPI-scorebord bevat een korte beschrijving van elke KPI en de resultaten op 31 december 2022. Deze resultaten worden vergeleken met de oorspronkelijke doelstellingen of met de resultaten van het voorgaande jaar, die als indicator worden gebruikt.

In 2022 hebben we - in sommige gevallen aanzienlijk - de doelstellingen bij acht van de negen KPI's gehaald of overtroffen; bij één KPI, namelijk KPI8 over de bezettingsgraad van de personeelsformatie, werd de doelstelling niet gehaald. Deze resultaten laten goed zien hoeveel voortgang we het hele jaar door hebben geboekt bij de uitvoering van onze strategische doelstellingen.

KERNPRESTATIE-INDICATOREN		Resultaten per 31.12.2022	Doelstelling 2022
KPI 1 Interne indicator	Aantal (mede) door de EDPS georganiseerde initiatieven, met inbegrip van publicaties, voor het toezicht op technologie en voor het bevorderen van technologieën ter verbetering van de privacy en gegevensbescherming	13 initiatieven	10 initiatieven
KPI 2 Interne & externe indicator	Aantal activiteiten gericht op interdisciplinaire beleidsoplossingen (intern & extern)	8 activiteiten	8 activiteiten
KPI 3 Interne indicator	Aantal in het kader van internationale samenwerking behandelde zaken (GPA, Raad van Europa, OESO, GPEN, IWGDPT, voorjaarsconferentie, internationale organisaties) waarvoor de EDPS een belangrijke schriftelijke bijdrage heeft geleverd	27 zaken	5 zaken
KPI 4 Externe indicator	Aantal dossiers waarvoor de EDPS in het kader van het EDPB als leidende rapporteur, rapporteur of lid van het redactieteam optrad	21 zaken	5 zaken

KPI 5 Externe indicator	Aantal adviezen uit hoofde van artikel 42 en gezamenlijke EDPS-EDPB-adviezen die zijn uitgebracht naar aanleiding van verzoeken van de Europese Commissie om legislatieve raadpleging	4 gezamenlijke adviezen 27 adviezen	Vorig jaar als benchmark
KPI 6 Externe indicator	Aantal fysieke of op afstand uitgevoerde audits/bezoeken	4 audits 2 bezoeken	3 verschillende audits/bezoeken
KPI 7 Externe indicator	Aantal volgers op de socialemedia-accounts van de EDPS: YouTube (YT), LinkedIn (L), Twitter (T), EU Voice en EU Video	YT - 2 750 L - 63 000 T - 29 100 EU Voice - 5 100 EU Video - 690	Resultaten van het voorgaande jaar + 10 %
KPI 8 Interne indicator	Bezettingsgraad van de personeelsinformatie	86,9%	90%
KPI 9 Interne indicator	Uitvoering van de begroting	98,2%	85%



edps.europa.eu



Bureau voor publicaties
van de Europese Unie

