Diverse wetten geven mensen het recht op inzage in de persoonsgegevens die organisaties van hen verwerken. Steeds meer mensen verzoeken ook om inzage. Veel organisaties hebben echter grote moeite om die inzage ookwerkelijk binnen de gestelde termijn te bieden. Michelle Wijnant en Jeroen van Helden geven handvatten om de afhandeling van de inzageverzoeken goed te laten verlopen.

door Michelle Wijnant en Jeroen van Helden beeld Shutterstock

Organisaties hebben interne behandeling van inzageverzoeken niet op orde

HET INZAGERECHT HOUDT DE GEMOEDEREN BEZIG. Juristen merken dat in hun praktijk en zien het terug in de jurisprudentie en activiteiten van toezichthouders. Op zich niet vreemd dat mensen zich steeds meer bewust worden van de waarde van hun persoonsgegevens en het recht op privacy. In de praktijk blijkt echter dat veel organisaties de interne behandeling van inzageverzoeken nog niet goed op orde hebben. Dit resulteert in het niet kunnen halen van de wettelijke termijnen, het bevragen van veel interne medewerkers, en zelfs juridische procedures en boetes. Recent kreeg Spotify een boete van maar liefst €5 miljoen. Dat moet anders kunnen. Daarom delen wij hier de tien belangrijkste aandachtspunten voor een soepele en efficiënte afhandeling van inzageverzoeken.

1) De relevante inzagerechten

Een persoon kan een inzagerecht hebben op alle persoonsgegevens die van hem of haar worden verwerkt op basis van de algemene privacywet, de Algemene Verordening Gegevensbescherming (AVG), maar ook op basis van specifieke wet- en regelgeving, zoals de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) of de Jeugdwet (Jw). Het is belangrijk dat u helder voor ogen heeft welke inzagerechten voor u relevant zijn. Wij zullen ons in dit artikel beperken tot de AVG.

2) De termijnen

Zodra een inzageverzoek binnenkomt, begint de teller te lopen. Vanaf het moment dat u het verzoek via de officiële kanalen heeft ontvangen (ongeacht of het een avond, weekend- of werkdag is), heeft u namelijk een maand de tijd om eraan te voldoen, of om te laten weten dat u een verlenging nodig heeft.
Bij complexe verzoeken (bijvoorbeeld wanneer het gaat om een jarenlang opgebouwd dossier) mag u deze termijn met twee maanden verlengen. U mag deze termijn ook verlengen – naar rato – als aanvullende informatie van de verzoeker nodig is (bijvoorbeeld voor identificatie of om precies te begrijpen wat de verzoeker wenst) en het vrij lang duurt voordat de verzoeker reageert.[1]

3) Locatie voor ontvangst van de inzageverzoeken

Medewerkers moeten weten van het bestaan van het recht van inzage, hoe inzageverzoeken kunnen binnenkomen en wat ze hiermee moeten doen. Daarnaast moet richting de personen wiens persoonsgegevens u verwerkt, worden gecommuniceerd waar ze hun verzoeken kunnen indienen. Ontvangt u een verzoek ontvangt via een ander kanaal dan u heeft aangegeven, betekent dit niet dat u het verzoek niet in behandeling hoeft te nemen.

4) Rollen en bevoegdheden

Intern dient u vast te leggen welke medewerkers inzageverzoeken mogen behandelen, hierover contact mogen hebben met de verzoekers, wie om input moet worden gevraagd voor de afweging en wie uiteindelijk het besluit mag nemen om (gedeeltelijk) wel of niet aan het verzoek te voldoen. Het is goed om ook al na te denken over afdelingen/functies die uw medewerkers moeten betrekken wanneer de verzoeker bijvoorbeeld klaagt over de behandeling van het verzoek.

5) Locatie van de persoonsgegevens

Om snel een inzageverzoek in behandeling te kunnen nemen, is het nodig om te weten waar de persoonsgegevens zich (kunnen) bevinden. Het is handig om dit in kaart te brengen door: 1) vast te stellen van welke categorieën personen u de persoonsgegevens verwerkt (zoals medewerkers, klanten, leveranciers); 2) welke systemen u hiervoor gebruikt; en 3) aan welke derde partijen (zoals leveranciers, samenwerkingspartners, vervoersbedrijven) u persoonsgegevens doorgeeft. Dit overzicht dient u vervolgens steeds up-to-date te houden, waarvoor iemand dus verantwoordelijk moet worden gemaakt. Een alternatief is om voor deze informatie te leunen op het verwerkingsregister of om gebruik te (gaan) maken van een data governance tool.

6) Identificatie van de verzoeker

Om zeker te weten dat de verzoeker is wie hij/zij zegt dat hij/zij is, moet de verzoeker worden geïdentificeerd. Het advies is om te werken met twee factoren voor deze identificatie. Denk hierbij aan het vragen naar een geboortedatum en volledige naam wanneer de contactgegevens die worden gebruikt door de verzoeker overeenkomen met uw administratie.

Hoe zwaar u de identificatieplicht maakt, moet afhangen van de gevoeligheid van de persoonsgegevens die worden gevraagd. Uit de boete die in 2022 door de Autoriteit Persoonsgegevens werd opgelegd aan DPG Media blijkt dat niet standaard een kopie van een ID-bewijs mag worden gevraagd.[2]

7) Communicatie met de verzoeker

Om te zorgen dat door de gehele organisatie op eenzelfde manier met verzoekers wordt gecommuniceerd, is het handig om een aantal templates beschikbaar te stellen. Denk hierbij aan

een standaard ontvangstbevestiging (inclusief identificatie), bericht bij niet-bevoegdheid[3] en berichten voor de (gedeeltelijke) opvolging of afwijzing van een verzoek. Daarnaast is het belangrijk om te overwegen of u, gezien de gevoeligheid van de persoonsgegevens die u verwerkt, het nodig acht om standaard een gesprek te voeren met verzoekers.

8) Afwegingen om wel/niet (of deels) aan een verzoek te voldoen

Dit aandachtspunt levert in de praktijk de grootste uitdaging op. Hier komen we namelijk op grijs gebied terecht doordat een belangenafweging gemaakt moet worden. De hoofdregel is dat aan een inzageverzoek moet worden voldaan, tenzij. De uitzonderingen kunnen worden afgeleid uit de AVG en aanverwante wet- en regelgeving, maar ook uit jurisprudentie of specifieke wetgeving waarop het verzoek is gebaseerd.

Zo mag een inzageverzoek worden afgewezen als het ziet op persoonsgegevens die alleen worden verwerkt voor, kort samengevat, wetenschappelijk onderzoek, journalistieke doeleinden of artistieke uitdrukkingsvormen. Ook de privacy van anderen dan de verzoeker of de zorg van een goed hulpverlener kunnen in de weg staan bij het geven van inzage. Welke 'tenzij' voor u relevant is, hangt met name af van de verwerkingen die u met de persoonsgegevens verricht en de wettelijke kaders die op u van toepassing zijn. Een zorgvuldige en gedocumenteerde belangenafweging is cruciaal.

9) Voldoen aan een verzoek

Als u heeft besloten om (gedeeltelijk) aan een verzoek te voldoen, dan moet u aan de betrokkene een kopie van de persoonsgegevens verstrekken samen met een toelichting.[4] De kopie kunt u verstrekken door de bestanden of docu-

menten waarin de persoonsgegevens zijn opgenomen te kopiëren of door alle persoonsgegevens in een (bijvoorbeeld Excel) bestand te plaatsen. Recent is geoordeeld dat er niet met een bestand kan worden volstaan als voor de verzoeker kopieën van dossiers, documenten of e-mails nodig zijn om de context waarin zijn/haar persoonsgegevens worden verwerkt te kunnen begrijpen.[5] Daarnaast is recent geoordeeld dat u in beginsel verplicht bent om in de toelichting de identiteit van derde partijen (naam organisatie) te noemen aan wie u de persoonsgegevens heeft doorgegeven. Het is overigens niet nodig om de namen van specifieke interne medewerkers te noemen.[6] Verder blijkt uit een recent boetebesluit van de Zweedse toezichthouder aan Spotify dat de toelichting volledige informatie moet bevatten over o.a. de bron van de persoonsgegevens, de ontvangers en de internationale data doorgifte.[7] Als u (gedeeltelijk) niet aan een verzoek voldoet, is het nodig dat u uitlegt waarom niet en dat u de verzoeker wijst op zijn/haar recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP) en beroep in te stellen bij de rechter (let op: u bent dit wettelijk verplicht!).

10) Interne registratie

We horen u bijna denken… zijn we er nu nog niet? Jawel, u bent er bijna. Het enige aandachtspunt dat u nog rest is de interne registratie. Het is van belang dat u documenteert welk verzoek u heeft ontvangen, hoe de verzoeker is geïdentificeerd, hoe op het verzoek is gereageerd en wat de afwegingen zijn geweest. Deze informatie kunt u namelijk nodig hebben voor eventuele audits, onderzoeken of vervolgprocedures.

Wanneer u voor de identificatie van een verzoeker een kopie ID heeft gebruikt die u nog niet bezat, sla deze kopie dan niet op maar noteer alleen de wijze (datum, kanaal, door wie, etc.) waarop de identificatie heeft plaatsgevonden.

voetnoten

[1] European Data Protection Board (EDPB), 'Guidelines 01/2022on data subject rights - Right of access', Version 1.0, 18 January 2022, punt 157-159.

[2] Autoriteit Persoonsgegevens, 'Boetebesluit DPG Media', 14 januari 2022 (URL: https://www.autoriteitpersoonsgegevens.nl/uploads/imported/boetebesluit...).

[3] In principe mag alleen de betrokkene zijn/haar wettelijke rechten uitoefenen ten aanzien van zijn/haar eigen persoonsgegevens. Een vertegenwoordiger kan echter op basis van de wet (zoals een ouder of voogd voor een kind of de nabestaanden van een overleden persoon), op basis van een rechterlijke aanwijzing (mentor of curator) of op basis van een schriftelijke machtiging (vertegenwoordiger of advocaat) gemachtigd zijn om dit namens de betrokkene te doen.

[4] In de toelichting moet o.a. worden vermeld waar de persoonsgegevens worden verwerkt, voor welke doeleinden dit gebeurt, waar ze vandaan komen, aan wie ze worden doorgegeven en hoe lang ze worden bewaard.

[5] HvJ EU 4 mei 2023, ECLI:EU:C:2023:369.

[6] HvJ EU 12 januari 2023, ECLI:EU:C:2023:3 en Conclusie AG 15 december 2022, ECLI:EU:C:2022:1001.

[7] Integritetsskydds Myndigheten, 'Beslut efter tillsyn enligt dataskyddsförordningen – Spotify AB', 12 juni 2023 (URL: https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-spotify.pdf).

Jeroen van Helden is advocaat IT, Privacy & Cybersecurity bij De Clercq Advocaten Notariaat, te Leiden. Dagelijks adviseert en procedeert hij op het gebied van (internationale) privacy en dataprotectievraagstukken en IT-projecten.

Michelle Wijnant CISM, CIPM, CIPT en CIPP/E is advocaat IT, Privacy & Cybersecurity bij De Clercq Advocaten Notariaat, te Leiden. Michelle adviseert en ondersteunt onder meer CISO's en FG's bij de uitvoering van hun werkzaamheden.

Reacties en bijdragen

Voor reacties en nieuwe bijdragen van IT-experts:
Tanja de Vrede
020-2467230
t.d.vrede@agconnect.nl