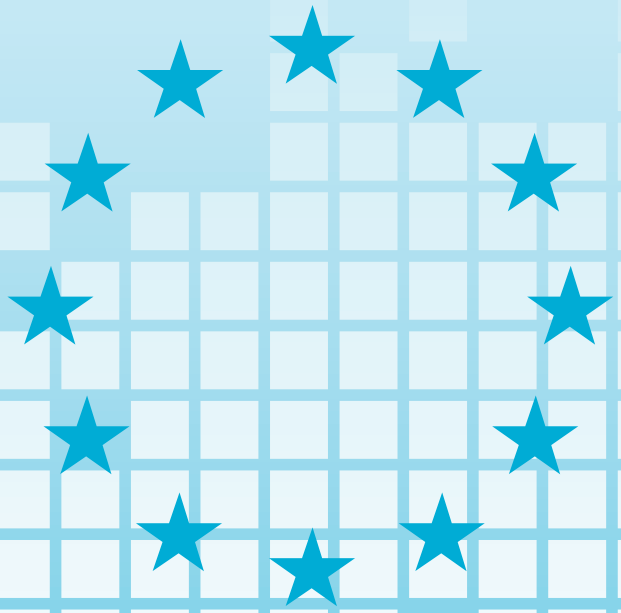
CBPL
Commissie voor de bescherming van de persoonlijke levenssfeer

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN



versie 2.0 (januari 2018)

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de regels rond verwerking van persoonsgegevens. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. REGISTER VAN VERWERKINGSACTIVITEITEN

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de gegevensbeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

4. COMMUNICATIE

Evalueer je bestaande privacyverklaring en bekijk deze in het licht van de AVG.

5. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

6. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

7. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

8. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

9. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

10. GEGEVENSLEKKEN

Voorzie adequate procedures om persoonlijke gegevenslekken op te sporen, te rapporteren en te onderzoeken.

11. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "*gegevensbescherming door ontwerp*" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

INTRO

ALGEMENE VERORDENING GEGEVENSBESCHERMING

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG) WORDT VAN TOEPASSING OP 25 MEI 2018. BEREID JE VOOR IN 13 STAPPEN!

Helemaal nieuw is de AVG natuurlijk niet! Veel van haar basisprincipes en concepten vonden we reeds terug in de Belgische Privacywet. Dus wie al voldeed aan deze wetgeving, heeft voor de implementatie van de AVG een voetje voor. Toch zijn er enkele nieuwigheden en aanzienlijke verbeteringen die de bestaande aanpak licht zullen wijzigen.

Met behulp van dit stappenplan, en de bijkomstige informatie op de website van de Privacycommissie, kan je een plan van aanpak opstellen. De Privacycommissie, i.s.m. de betrokkenen sectoren, geeft voortdurend bijkomende richtlijnen en instrumenten om bedrijven en organisaties te begeleiden bij deze voorbereiding. Op Europees Niveau heeft ook de Groep gegevensbescherming artikel 29 enkele richtlijnen uitgebracht. Het Europees Comité voor gegevensbescherming zet het werk verder.

Kijk ook om je heen – ga na of er modellen bestaan voor jouw sector of gedragscodes ontwikkeld zijn door sectorverenigingen. Verzeker je van de steun en medewerking van de sleutelfiguren in jouw organisatie. Zo moet je bijv. voorzien in procedures om te voldoen aan de vereisten van transparantie of om de rechten van de betrokkene te garanderen. In een groot bedrijf of complexe organisatiestructuur kan dit aanzienlijke gevolgen teweegbrengen op het vlak van budget, IT, personeel, beleid en communicatie.

Een klemtoon van de AVG is de documentatieplicht van de verwerkingsverantwoordelijke, als blijk van diens verantwoordelijkheid. Dit stappenplan helpt bedrijven en organisaties hun huidig gegevensbeschermingsbeleid te evalueren en aan te passen aan de vereisten van de AVG. Een eerste stap hierin kan zijn om de bestaande contracten en regelingen voor gegevensuitwisseling te herzien.

Houd er rekening mee dat sommige bepalingen uit de AVG meer impact zullen hebben op jouw bedrijf of organisatie, dan andere, zoals bijv. de bepalingen inzake profilering of de specifieke beschermingsregels voor persoonsgegevens van kinderen. Het kan dus nuttig zijn om nu reeds in kaart te brengen welke bepalingen van de AVG de grootste impact zullen hebben op jouw bedrijf of organisatie, en deze bij voorkeur eerst door te voeren.

BEWUSTMAKING

1

Zorg dat de sleutelfiguren en beleidsmakers in jouw bedrijf of organisatie op de hoogte zijn van de regelgeving. Zij moeten de gevolgen hiervan inschatten en aanwijzen welke domeinen vandaag mogelijks problematisch kunnen zijn in het licht van de AVG. Indien jouw bedrijf of organisatie over een risicoregister beschikt, kan dit een werkbaar vertrekpunt zijn.

Het implementeren van de AVG kan een behoorlijke invloed hebben op de beschikbare middelen, zeker voor wat betreft grote en meer complexe bedrijven of organisatiestructuren. Ga na of er voor jouw sector modellen bestaan of gedragscodes ontwikkeld werden door de sectorverenigingen.

REGISTER VAN VERWERKINGSACTIVITEITEN

2

Breng zorgvuldig in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Je doet er goed aan al je verwerkingen te registreren. Mogelijks dien je hiervoor een informatie-audit te organiseren. Dit kan dan van het volledige bedrijf of enkel van welbepaalde afdelingen.

De AVG geeft de betrokkenen een aantal rechten, specifiek op maat van de netwerkwereld. Wanneer jouw bedrijf bijv. onnauwkeurige persoonsgegevens bijhoudt, en heeft gedeeld met andere organisaties, zal je deze laatste moeten inlichten over de onnauwkeurigheid zodat deze een correctie kan aanbrengen in haar eigen gegevens. Deze documentatieplicht helpt je bovendien de verantwoordelijkheidsvereiste uit de AVG na te leven. Volgens dit principe dient een bedrijf of organisatie te bewijzen dat ze in overeenstemming met de gegevensbeschermingsprincipes handelt.

Om hierbij te helpen, stelt de Privacycommissie op haar website een modelregister van verwerkingsactiviteiten ter beschikking met een bijbehorende handleiding.

LEES OOK

- Aanbeveling 06/2017
- Model voor register van verwerkingsactiviteiten

FUNCTIONARIS VOOR GEGEVENSBESCHERMING

3

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de gegevensbeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

De AVG vereist voor sommige bedrijven en organisaties dat zij een functionaris voor gegevensbescherming aanwijzen, bijvoorbeeld voor openbare overheden of verwerkers wiens kerntaak bestaat uit het regelmatig en stelselmatig observeren op grote schaal van betrokkenen of een grootschalige verwerking van gevoelige gegevens.

LEES OOK

- Aanbeveling 04/2017
- Richtlijnen over de functionaris voor gegevensbescherming (WP243)

Het is van belang dat, hetzij iemand in de organisatie, hetzij een externe adviseur, verantwoordelijkheid neemt voor het naleven van de gegevensbeschermingsprincipes en dat iemand de kennis, medewerking en bevoegdheid heeft om dit te doen. Daarom moet je nu reeds beoordelen of op jouw bedrijf of organisatie de plicht rust een dergelijke functionaris aan te stellen. Zo ja, evalueer of de huidige aanpak in lijn is met de vereisten van de AVG.

COMMUNICATIE

Evalueer je bestaande privacyverklaring en bekijk deze in het licht van de AVG. Wanneer jouw bedrijf of organisatie persoonsgegevens verwerkt, dien je aan de betrokkene bepaalde informatie te verschaffen, zoals de identiteit van de verwerker en de wijze waarop die de gegevens zal aanwenden. Doorgaans wordt deze informatie verstrekt in de vorm van een privacyverklaring.

De AVG stelt inhoudelijke eisen aan deze privacyverklaring. Zo zal je de wettelijke grondslag voor de gegevensverwerking moeten meedelen, de termijnen gedurende dewelke je de informatie zal bijhouden, of je de gegevens uitwisselt buiten de Europese Unie en de mogelijkheid voor de betrokkene om een klacht in te dienen bij de toezichthoudende autoriteit indien deze meent dat zijn persoonsgegevens foutief worden verwerkt. De AVG vereist dat deze informatie wordt verschaft in beknopte, begrijpbare en duidelijke taal.

LEES OOK

- Richtlijnen over transparantie (WP260)

RECHTEN VAN DE BETROKKENE

Je dient na te gaan of de procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.
De AVG voorziet o.a. in de volgende rechten voor de betrokkene:

- ***Informatie en toegang tot persoonsgegevens***
- ***Correctie en uitwissing van de gegevens***
- ***Bezwaar tegen direct marketingpraktijken***
- ***Bezwaar tegen geautomatiseerde besluitvorming en profilering***
- ***Overdraagbaarheid van de gegevens***

Zorg voor draaiboeken die uitstippelen wat te doen wanneer iemand zijn of haar recht wil uitoefenen. Wie neemt de beslissing? Zijn je systemen hiertoe uitgerust? Het recht op overdraagbaarheid van de gegevens verdient bijzondere aandacht. Dit is een versterkte vorm van toegang waarbij de betrokkene het recht heeft de persoonsgegevens die op hem van toepassing zijn in een gestructureerde, gangbare en elektronische vorm te verkrijgen. De meeste bedrijven en organisaties deden dit al, maar let er op dat papieren print-outs of een ongebruikelijke elektronische vorm niet volstaan voor de AVG.

Doe je aan geautomatiseerde individuele besluitvorming? Wees je dan bewust van de bijzondere spelregels die hiervoor gelden onder de AVG.

LEES OOK

- Richtlijnen over de overdraagbaarheid van gegevens (WP242)
- Richtlijnen over geautomatiseerde individuele besluitvorming (WP251)

VERZOEK TOT TOEGANG

6

Bedenk hoe je verzoeken tot toegang zal behandelen onder de termijnen in de AVG en voorzie eventueel een update van je bestaande toegangsprocedures.

De AVG legt vast hoe met toegangsverzoeken om te gaan. In de meeste gevallen moet gratis en binnen de 30 dagen gevolg worden gegeven aan het verzoek tot toegang. Manifest ongegronde of overmatige verzoeken kunnen worden aangerekend of worden geweigerd. Indien jouw bedrijf of organisatie in staat wil zijn om toegangsverzoeken te weigeren, moet je daarvoor een beleid en aangepaste procedures hebben.

Je dient de betrokkene die om toegang verzoekt bepaalde bijkomstige informatie te verschaffen, zoals de termijnen gedurende dewelke je informatie bijhoudt en het recht om onnauwkeurige gegevens te laten verbeteren. Indien jouw bedrijf of organisatie een groot aantal toegangsverzoeken behandelt, is een goed draaiboek cruciaal. Het moet logistiek mogelijk zijn om alle verzoeken binnen de voorziene tijdspanne te verwerken en de betrokkene van de noodzakelijke informatie te voorzien. Hierover moet zorgvuldig worden nagedacht.

Op termijn kan het kostenbesparend zijn een systeem te ontwikkelen dat de betrokkene in staat stelt de gegevens zelf online te raadplegen. Bedrijven en organisaties worden aangespoord een kosten/baten analyse uit te voeren van een dergelijk online toegangssysteem.

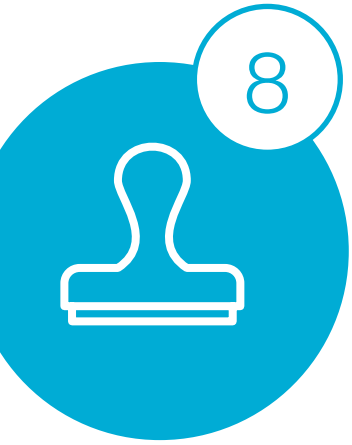
WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

7

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen. Je moet kiezen uit de grondslagen opgesomd in de AVG, maar let op het verschil tussen ‘gewone’ en ‘bijzondere’ gegevens.

Onder de AVG kunnen de rechten van de betrokkene variëren naargelang de wettelijke basis van de gegevensverwerking. Het meest voor de hand liggende voorbeeld is dat de betrokkene een sterker recht heeft om de verwijdering van zijn gegevens te vragen indien zijn toestemming aan de grondslag lag voor de verwerking.

Het is belangrijk om de gekozen wettelijke grondslag voor de gegevensverwerking te verduidelijken in de privacyverklaring en telkens wanneer je een toegangsverzoek beantwoordt. Kijk dus na welke gegevensverwerkingen je uitvoert; bepaal de wettelijke basis en documenteer dit zorgvuldig in het licht van de verantwoordelijkheidsvereiste.



TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert. De AVG vermeldt “toestemming” en “expliciete toestemming”. Het onderscheid maken is niet nodig, aangezien de toestemming in beide gevallen vrij, specifiek, geïnformeerd en ondubbelzinnig moet zijn. De toestemming moet ook blijken uit een actieve indicatie van akkoord. M.a.w. de toestemming kan niet worden afgeleid uit een stilzwijgen, een vooraf aangevinkt vakje of uit een niet-handelen. Indien je rekent op de toestemming van de betrokkene om diens gegevens te verwerken, zorg dan zeker dat die toestemming voldoet aan de vereisten van de AVG. Noteer dat de toestemming controleerbaar moet zijn en dat de betrokkene doorgaans meer rechten heeft wanneer je vertrouwt op toestemming als grondslag voor de gegevensverwerking.

De AVG verduidelijkt dat de verwerkingsverantwoordelijke in staat moet zijn om aan te tonen dat toestemming werd gegeven. Evalueer dus je systemen die toestemming registreren, teneinde te verzekeren van een effective audit trail (controlespoor).

LEES OOK

- Richtlijnen over toestemming (WP259)

KINDEREN

De AVG laat in één bepaalde context kinderen vanaf 16 jaar toe om zelf toe te stemmen met gegevensverwerking, namelijk in de context van commerciële internetdiensten die zich rechtstreeks richten tot kinderen.

Let op – de Belgische wetgever mag de groep 13 - 16-jarigen hetzelfde privilege geven – hou de berichtgeving van de Privacycommissie in het oog. Let wel op, kinderen die zelf toestemden mogen eisen dat hun gegevens op elk moment gewist worden, ook na hun meerderjarigheid!

Bekijk of je gegevens verwerkt van minderjarige kinderen en of je de leeftijd van de betrokkene moet nagaan. Ga na hoe je met de ouder(s) of voogd(en) in contact kan treden, bijvoorbeeld om toestemming te vragen of een contract aan te gaan.

Indien jouw bedrijf of organisatie gegevens van kinderen verzamelt, hou rekening met de rol die hun ouders of voogd spelen! Onthoud dat de toestemming controleerbaar moet zijn en dat desgevallend de privacyverklaring moet geschreven zijn in voor kinderen begrijpbare taal.

GEGEVENSLEKKEN

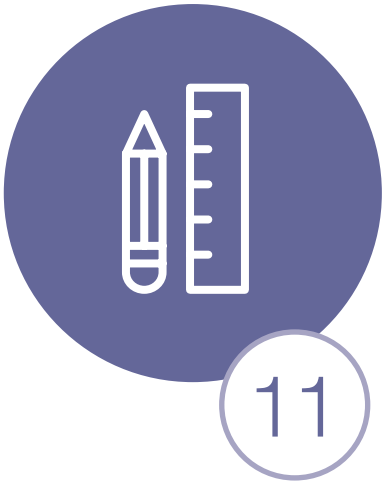
Voorzie adequate procedures om persoonlijke gegevenslekken op te sporen, te rapporteren en te onderzoeken. Beoordeel hiervoor de verscheidene types van persoonsgegevens die je bijhoudt en documenteer welke binnen de meldingsplicht zouden vallen, ingeval zich een gegevenslek zou voordoen. In sommige gevallen moet je de betrokkene die het voorwerp uitmaakt van het gegevenslek rechtstreeks verwittigen, bv. wanneer het lek aanleiding kan geven tot persoonlijke financiële verliezen. Grotere bedrijven of organisaties zullen een beleid en procedures moeten ontwikkelen om gegevenslekken te beheren – hetzij op centraal, hetzij op lokaal niveau.

Niet alle gegevenslekken zullen moeten worden gemeld aan de toezichthoudende autoriteit – enkel deze waarbij het waarschijnlijk is dat de betrokkene enige vorm van schade zal leiden, bv. als gevolg van een identiteitsdiefstal of het schenden van een geheimhoudingsplicht. Noteer dat de niet naleving van de meldplicht kan resulteren in een geldboete, bovenop de boete voor het gegevenslek zelf.

LEES OOK

- Richtlijnen over de melding van gegevenslekken (WP250)

GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGS-EFFECTBEOORDELING (GEB)



Maak je vertrouwd met de begrippen “gegevensbescherming door ontwerp” en “gegevensbeschermingseffectbeoordeling”, beter gekend als *Privacy by design* en *Data Protection Impact Assessment (DPIA)*. Ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren. Deze kunnen worden gelinkt aan andere organisatorische processen zoals risicobeheer en projectbeheer. Beoordeel de situaties waarin het nodig is dergelijke analyses uit te voeren. Wie zal dit doen? Wie moet hierbij worden betrokken? Gebeurt de analyse centraal of lokaal? Het behoorde altijd al tot de “good practices” van een bedrijf of organisatie om gegevensbescherming van bij de start in te bouwen en als onderdeel hiervan een effectbeoordeling uit te voeren. De AVG maakt hiervan een duidelijke wettelijke vereiste.

Noteer dat je niet steeds een GEB moet uitvoeren. Deze is enkel vereist in hoge risicosituaties, bijv. wanneer een nieuwe technologie wordt geïmplementeerd of wanneer een profileringsoperatie een aanzienlijk effect kan teweegbrengen voor de betrokkenen. Wanneer de GEB aangeeft dat de gegevensverwerking een “hoog risico” inhoudt en dit ondanks maatregelen genomen ter beheersing van het “hoog risico” (met andere woorden er is een “hoog residueel risico”), is het noodzakelijk het advies in te winnen van de toezichthoudende autoriteit omtrent de wetmatigheid van de verwerking in het licht van de AVG.

LEES OOK

- Aanbeveling uit eigen beweging 01/2018
- Richtlijnen over de GEB (WP248)

INTERNATIONAAL

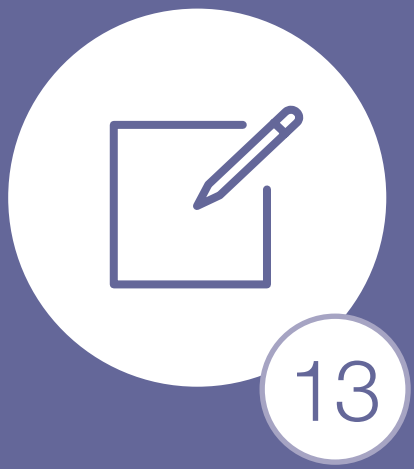
Indien jouw bedrijf of organisatie internationaal actief is, dien je te bepalen onder welke toezichthoudende autoriteit je valt. De AVG voorziet een enigszins complexe regeling om te bepalen welke toezichthoudende autoriteit de leiding neemt bij het onderzoek naar een klacht met een internationaal karakter, bijv. wanneer een gegevensverwerking betrekking heeft op inwoners van meerdere lidstaten. De leidende autoriteit wordt bepaald naargelang waar het bedrijf of de organisatie haar hoofdvestiging heeft of de vestiging waar de beslissingen omtrent de gegevensverwerkingen worden genomen. Voor een traditionele hoofdzetel is dit vrij eenvoudig vast te stellen. Moeilijker wordt het voor complexe, multi-site bedrijven of organisaties waarbij beslissingen omtrent diverse verwerkingsactiviteiten op verschillende plaatsen worden genomen.

Om duidelijkheid te krijgen over welke toezichthoudende autoriteit de leiding heeft over jouw bedrijf of organisatie kan het raadzaam zijn in kaart te brengen waar jouw organisatie haar meest belangrijke beslissingen omtrent gegevensverwerkingen neemt. Dit zal je helpen bij het bepalen van jouw “hoofdvestiging” en dus ook van de bevoegde toezichthoudende autoriteit.

LEES OOK

- Richtlijnen over de leidende toezichthoudende autoriteit (WP244)

BESTAANDE CONTRACTEN



Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng indien nodig veranderingen aan. De AVG creëert een intelligent systeem die de verhouding tussen de verwerkingsverantwoordelijke en de verwerkers behelst. Het bepaalt zelfs de voorwaarden die van toepassing zijn op onder-aanneming activiteiten. Opdat je deze voorwaarden zou aantreffen, moet je bestaande contracten beoordelen en de nodige wijzigingen aanbrengen.

De AVG benadrukt het belang van op databanken toepasselijke veiligheidsmaatregelen. Ook in het geval van outsourcing is het belangrijk te beoordelen of de veiligheidsmaatregelen die werden voorzien in de bestaande contracten nog steeds toereikend zijn en voldoen aan de vereisten van de AVG.

MEER INFORMATIE OVER DE ALGEMENE VERORDENING GEGEVENSBESCHERMING VINDT U IN HET THEMADOSSIER OP ONZE WEBSITE: WWW.PRIVACYCOMMISSION.BE

Commissie voor de bescherming van de persoonlijke levenssfeer

Drukpersstraat 35 | B-1000 Brussel | T+32 (0)2 274 48 00
E-mail: commission@privacycommission.be
Website: https://www.privacycommission.be

Verantwoordelijke uitgever
W. Debeuckelaere
Druk
Centrale drukkerij van de Kamer van volksvertegenwoordigers
Vormgeving
The Reference

Er bestaat ook een Franse en Engelse versie van dit stappenplan.
Il existe aussi une version française et anglaise de ce plan par étapes.
U kunt dit stappenplan ook raadplegen of downloaden op
de website van de Privacycommissie.