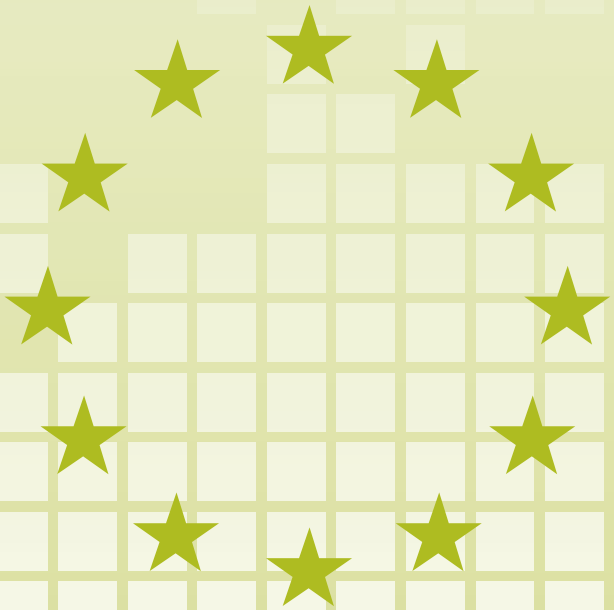
ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN



CBPL
Commissie voor de bescherming van de persoonlijke levenssfeer

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

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. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. 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.

5. VERZOEK TOT TOEGANG

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

6. 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.

7. TOESTEMMING

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

8. 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.

9. DATALEKKEN

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

10. 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.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

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

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

DE ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG) IS OP 24 MEI 2016 IN WERKING GETREDEN. BEDRIJVEN EN ORGANISATIES KRIJGEN EVENWEL TOT 25 MEI 2018 DE TIJD OM ZICH AAN DE NIEUWE REGELGEVING AAN TE PASSEN. BEREID JE VOOR IN 13 STAPPEN!

Helemaal nieuw is de AVG natuurlijk niet! Veel van haar basisprincipes en concepten vinden we reeds terug in de actuele Belgische Privacywet. Dus wie vandaag al voldoet aan de huidige wetgeving, zal deze benadering als geldig uitgangspunt kunnen nemen voor de implementatie van de AVG. Toch zijn er enkele nieuwigheden en aanzienlijke verbeteringen die de huidige aanpak licht zullen wijzigen.

Met behulp van deze handleiding, en de bijkomstige informatie op de website van de Privacycommissie, kan je de verschillen tussen de huidige Privacywet en de nieuwe AVG opsporen en je beleid hierop afstemmen. In de komende maanden zal de Privacycommissie, i.s.m. de betrokkenen sectoren, bijkomende richtlijnen en instrumenten uitwerken om bedrijven en organisaties te begeleiden bij deze voorbereiding. Op Europees Niveau zal de Groep gegevensbescherming artikel 29 de nodige bijstand verlenen.

Belangrijk is om nu reeds voorbereidingen te treffen om de overgang naar de nieuwe regelgeving vlot te laten verlopen. Verzeker je hierbij van de steun en medewerking van de sleutelfiguren in jouw organisatie. Zo moet je bijv. voorzien in nieuwe 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.

De AVG legt meer nadruk op de documentatieplicht van de verwerkingsverantwoordelijke, als blijk van diens verantwoordelijkheid. Deze handleiding helpt bedrijven en organisaties hun huidig databeschermingsbeleid te evalueren en aan te passen aan de nieuwe 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.

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEWUSTMAKING

Zorg dat de sleutelfiguren en beleidsmakers in jouw bedrijf of organisatie op de hoogte zijn van de nieuwe 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. Gebruik de tweejarige overgangsperiode dus allereerst om medewerkers te informeren over de aankomende veranderingen. Stel dit niet uit tot de laatste minuut.

DATAREGISTER

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 introduceert enkele vernieuwde 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 register.
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 databeschermingsprincipes handelt.

COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.
Wanneer jouw bedrijf of organisatie nu reeds 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 vereist dat deze privacyverklaring wordt aangevuld met nieuwe informatietypes. Zo zal je voortaan 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 Privacycommissie indien deze meent dat zijn persoonsgegevens foutief worden verwerkt.
De AVG vereist dat deze informatie wordt verschaft in beknopte, begrijpbare en duidelijke taal.

RECHTEN VAN DE BETROKKENE

Je dient na te gaan 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. 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***

Meer algemeen, geniet de betrokkene onder de AVG dezelfde rechten als onder de huidige Belgische Privacywet, mits enkele aanzienlijke verbeteringen. Indien jouw bedrijf of organisatie nu reeds voldoende is uitgerust om in deze individuele rechten te voorzien, dan zal de overgang naar de AVG relatief vlot verlopen. Het is nu een goed moment om jouw bestaande procedures te evalueren en na te gaan hoe je voortaan te werk zal gaan wanneer iemand zijn of haar recht wil uitoefenen. Wie neemt de beslissing? Zijn je systemen hiertoe uitgerust?
Het recht op overdraagbaarheid van de gegevens is een nieuwigheid. Dit is een verbeterde 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 doen dit al, maar indien je nog steeds gebruik maakt van papieren print-outs of een ongebruikelijke elektronische vorm, dan is het nu een goed moment om dit te herzien.

VERZOEK TOT TOEGANG

Voorzie een update van je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.
De AVG voorziet nieuwe regels over hoe met toegangsverzoeken om te gaan. In de meeste gevallen zal gratis en binnen de 30 dagen (i.t.t. de huidige termijn van 45 dagen) gevolg moeten 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, dien je het beleid en de procedures dusdanig aan te passen.
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 zullen de wijzigingen die de AVG voorziet een aanzienlijke impact teweeg brengen. 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

6

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.
Veel bedrijven en organisaties hebben destijds wellicht geen wettelijke grondslag bepaald voor de gegevensverwerkingen die ze uitvoeren. Onder de huidige wetgeving heeft dit weinig of geen praktische gevolgen. Dit verandert evenwel onder de AVG omdat de rechten van de betrokkene kunnen 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. De wettelijke grondslagen in de AVG zijn quasi identiek aan deze in de huidige Privacywet. 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, en wijzig waar nodig.
De AVG vermeldt “toestemming” en “expliciete toestemming”. Het onderscheid is niet echt duidelijk, 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. Indien dit nu nog niet het geval is, wijzig dan je toestemmingsmechanisme of ga op zoek naar een alternatief voor toestemming als grondslag voor de gegevensverwerking. Noteer dat de toestemming controleerbaar moet zijn en dat de betrokkene doorgaans meer rechten heeft wanneer je vertrouwd 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 de huidige systemen die toestemming registreren, teneinde een audit trail (controlespoor) te verzekeren

7

ALGEMENE VERORDENING GEGEVENSBESCHERMING

8

KINDEREN

Start vandaag met de ontwikkeling van 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. Voor het eerst zal de AVG speciale bescherming bieden aan de persoonsgegevens van kinderen, in het bijzonder in de context van commerciële internetdiensten zoals sociale netwerken. Kortweg, indien jouw bedrijf of organisatie gegevens van kinderen – onder de 16 jaar – verzamelt, zal een ouder of voogd toestemming moeten geven opdat de gegevensverwerking rechtmatig zou zijn. Dit kan aanzienlijke gevolgen teweeg brengen indien jouw bedrijf of organisatie gericht is op het aanbieden van diensten aan kinderen en als dusdanig hun persoonsgegevens verzamelt. Onthoud dat de toestemming controleerbaar moet zijn en dat desgevallend de privacyverklaring moet geschreven zijn in voor kinderen begrijpbare taal.

9

DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken 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 datalek zou voordoen. In sommige gevallen moet je de betrokkene die het voorwerp uitmaakt van het datalek 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 datalekken te beheren – hetzij op centraal, hetzij op lokaal niveau.
Niet alle datalekken zullen moeten worden gemeld aan de Privacycommissie – 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 datalek zelf.

10

GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGS-EFFECTBEOORDELING

Maak je nu reeds vertrouwd met de begrippen “gegevensbescherming door ontwerp” en “gegevensbeschermingseffectbeoordeling”, beter gekend als Privacy by design en Privacy impact assessment (PIA). 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 nu reeds die situaties waarin het nodig zal zijn dergelijke analyses uit te voeren. Wie zal dit doen? Wie moet hierbij worden betrokken? Gebeurt de analyse centraal of lokaal?
Het behoort 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. Dit was voordien slechts een impliciete vereiste van de databeschermingsprincipes. De AVG maakt hiervan een duidelijke wettelijke vereiste.
Noteer dat je niet steeds een effectbeoordeling 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 PIA aangeeft dat de gegevensverwerking een “hoog risico” inhoudt, is het noodzakelijk het advies in te winnen van de Privacycommissie omtrent de wetmatigheid van de verwerking in het licht van de AVG.

FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. 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 taak bestaat uit het regelmatig en stelselmatig observeren van betrokkenen op grote schaal. Het is van belang dat, hetzij iemand in de organisatie, hetzij een externe adviseur, verantwoordelijkheid neemt voor het naleven van de databeschermingsprincipes 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.

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.

BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke 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 DE WEBSITE VAN DE PRIVACYCOMMISSIE (NL)

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: http://www.privacycommission.be

Verantwoordelijke uitgever
W. Debeuckelaere
Druk
Centrale drukkerij van de Kamer van volksvertegenwoordigers
Vormgeving
Design is Dead

Er bestaat ook een Franse versie van deze handleiding.
Il existe aussi une version française de ce manuel.
U kunt deze brochure ook raadplegen of downloaden op de website van de Privacycommissie.