Overzicht Europese Algemene Verordening Gegevensbescherming

Boete tot €20.000.000 of tot 4 % van de jaarlijkse wereldwijde omzet in het geval van een onderneming, afhankelijk van welk bedrag hoger is

Gegevens

''mag het?'

Rechtmatig verkregen gegevens - grondslagen voor rechtmatige verwerking: Ondubbelzinnige toestemming, noodzakelijk voor uitvoeren overeenkomst, wettelijke plicht, bescherming vitale belangen, taak van algemeen belang, gerechtvaardigd belang. Laatste grond geldt niet langer voor overheid in het uitvoeren van hun taak.	6 8
Beginselen van toepassing op verwerking van persoonsgegevens: Rechtmatigheid, eerlijkheid en transparantie, gespecificeerde, expliciete en rechtmatige doelbinding, minimale gegevensverwerking en opslag, juistheid, doeltreffendheid, integriteit en verantwoordingsplicht.	5 6-11
Aantoonbare toestemming voor bepaalde doeleinden De bewijslast ligt bij de organisatie aan wie toestemming is verleend. Betrokkenen moeten deze toestemming altijd eenvoudig kunnen intrekken. Bepalingen die niet aan de regels voldoen zijn nietig. Toestemming moet op een duidelijke manier gevraagd worden en apart van andere zaken.	7 -
Doorgifte van persoonsgegevens Doorgifte buiten EU is slechts onder voorwaarden toegestaan. Multinationals kunnen bindende bedrijfsvoorschriften opstellen en door de nationale toezichthouder laten goedkeuren.	45-47 76-78
Bijzondere persoonsgegevens (o.a. etniciteit, gezondheid, seksuele voorkeuren) Het verwerken van bijzondere persoonsgegevens is niet toegestaan of er gelden strikte voorwaarden.	9 16
Extra bescherming voor kinderen onder de 16 jaar Verwerking van persoonsgegevens van kinderen jonger dan 16 jaar is alleen toegestaan na toestemming van een ouder of wettelijk vertegenwoordiger. Organisaties moeten zich redelijk inspannen om de toestemming te controleren, met het oog op de technische mogelijkheden hiervan.	8 -
Profilering ('profiling') Profilering met juridische gevolgen is slechts onder voorwaarden toegestaan. Profilering met aanzienlijke gevolgen voor betrokkenen moet gebaseerd zijn op menselijke beoordeling.	22
Uitzondering voor bepaalde doelen Historische, statistische of wetenschappelijke doeleinden zijn uitgezonderd.	5/89 17-23

Maintenance

'hoe ga je er mee om?'

Implementatie en documentatie Organisaties moeten o.a. analyseren welke verwerkingen worden uitgevoerd door henzelf of hun leveranciers, welke soorten gegevens het betreft, voor welke doeleinden zij dit doen en welke beveiligingsmaatregelen getroffen zijn.	5, 24
Checken, bekijken en sluiten bewerkersovereenkomsten Bewerkersovereenkomsten met leveranciers of afnemers zijn nodig in het geval persoonsgegevens worden verwerkt.	28/29 14
Risicoanalyses en PIA (DPIA/compliance review) Voor nieuwe en bestaande diensten moet een risico analyse worden uitgevoerd. Bij diensten/systemen met een hoog risico moet vervolgens een Privacy Impact Assessment worden uitgevoerd.	24/35 -
Informatiebeveiliging Organisaties moeten persoonsgegevens met passende technische en organisatorische maatregelen beveiligen.	24/32/ 35 13
Beheer van toestemming en rechten van betrokkenen Systemen en processen zullen moeten worden ingericht en beheerd om tegemoet te komen aan de rechten van betrokkenen. (Recht van inzage, rectificatie en het "recht om vergeten te worden")	7/15/16 /17/18/ 19 -
Dataportabiliteit Betrokkenen hebben het recht op een kopie van hun (persoons)gegevens in een elektronisch en bruikbaar formaat.	20 -
Aannemen beleid, implementeren technische en organisatorische maatregelen Organisaties moeten beleid opstellen en aantoonbaar technische en organisatorische maatregelen nemen om er voor te zorgen dat persoonsgegevens transparant en in overeenstemming met de regels worden verwerkt.	24/32
Bewaartermijn Beperk de opslagperiode en verwijder of archiveer (indien toegestaan) gegevens tijdig.	5/89 10

Organisatie

'hoe richt je de organisatie en processen in?'

Functionaris voor de gegevensbescherming / data protection officer Organisaties moeten in bepaalde gevallen een functionaris voor de gegevensbescherming aanstellen. Dit is het geval als het verwerken gedaan wordt door een publiek lichaam of autoriteit, als de corebusiness gegevens verwerken is, of als er grote hoeveelheden bijzondere gegevens verwerkt worden.	37/38 /39 62
Rechten van betrokkenen (inzage, correctie, verwijderen, compensatie, bezwaar) Implementeer processen voor het uitoefenen van rechten. Betrokkenen mogen informatie opvragen over: doel, categorieën persoonsgegevens, ontvangers, bewaartermijn, rechten van betrokkene, het recht om een klacht in te dienen en mogen bezwaar maken tegen profilering.	15/16 /17/2 1/22/ 24 35-42
Meldplicht datalekken Implementeer processen voor het melden van datalekken.	33/34 -
Getrainde medewerkers, een privacybewuste organisatie Om de risico's te minimaliseren moeten organisaties en hun medewerkers bewust zijn van de belangrijkste elementen van de regelgeving.	5/24/ 28 -
Privacy relevant voor ontwikkeling van producten en diensten (privacy by design/default) Weeg privacyaspecten mee bij het ontwikkelen van nieuwe producten en diensten.	25 -
Certificering De wetgeving stimuleert organisaties om certificering op het gebied van privacy te halen. Deze certificering mag door de toezichthouder of het nationaal accreditatie lichaam worden uitgegeven.	42/43 /83 -
Toezicht De toezichthouder in het land van de feitelijke hoofdvestiging van de organisatie zal verantwoordelijk zijn voor het toezicht.	56/60 -

Communicatie

'hoe communiceer je erover?'

Duidelijke en begrijpelijke communicatie over persoonsgegevens Informatie en communicatie moeten in een begrijpelijke vorm en in duidelijke (gewone) taal zijn opgesteld, zeker als deze zich richt tot kinderen.	7/8/14/ 15/21
Melden datalekken bij toezichthouder en betrokkenen Datalekken moeten binnen 72 uur aan de toezichthouder gemeld worden en in sommige gevallen is directe melding aan de betrokkene vereist. In gevallen waar het datalek niet gemeld is binnen 72 uur moet een met reden omklede melding gedaan worden bij de toezichthouder.	33/34 -
Contactgegevens functionaris voor de gegevensbescherming (FG) Contactgegevens van de FG moeten worden gepubliceerd en aan de toezichthouder worden gestuurd en betrokkenen moeten contact op kunnen nemen om hun rechten uit te oefenen.	37 63
Communicatie met de toezichthouder De toezichthouder mag documenten en gegevens opvragen en heeft de bevoegdheid om toegang te krijgen tot alle persoonsgegevens en de locaties waar deze zijn opgeslagen.	31/58 60
Bezwaar tegen profilering Betrokkenen moeten op een uiterst zichtbare manier expliciet worden geïnformeerd over de mogelijkheid om bezwaar te maken tegen profilering.	22