AVG: ALGEMENE VERORDENING GEGEVENSBESCHERMING ('GDPR') EN COMBELL

OMSCHRIJVING VAN CONFORMITEIT DOOR POLICY EN PRAKTISCH HANDELEN

Laatst bijgewerkt: 28 november 2017

COMBELL GROUP NV • Skaldenstraat 121 • B-9042 Gent • Tel: +32(0)9 218 79 79 • Fax: +32(0)9 270 30 60
www.combell.com • info@combell.com • KBC: 737-0036589-60 • IBAN BE73 7370 0365 8660 • BIC KREDBEBB
BTW: BE 0475.231.011 • Combell is ISO 9001:2000 certified and Microsoft Certified Partner

Inhoudsopgave

1 Introductie

1.1 Over de 'Algemene Verordening Gegevensbescherming'

De AVG (Engels: *GDPR*) is wetgeving die door de EU voor haar lidstaten is opgesteld om het verwerken van persoonlijke gegeven te reguleren. Het vervangt eerdere wetgeving die van vóór het Cloud-tijdperk stamt waarin grootschalige verzameling en 'mining' van data – waaronder persoonlijke data –gemeengoed is geworden. De wet beoogt de risico's van dergelijke 'Verwerking' te controleren.

Aan deze Europese wet liggen vier jaar van voorbereiding ten grondslag, waarin de Werkgroep *'Article 29'* de regelgeving inzake bescherming van persoonlijke informatie in lijn bracht met de nieuwe, onvoorziene manieren waarop data tegenwoordig wordt behandeld.

1.2 Wat is er nieuw, in vergelijking

Alle lidstaten van de EU hebben al hun eigen, lokale wetten inzake bescherming van data (veelal vormgegeven naar twee niet-dwingende Directieven van de EU: de *Data Protection Act* uit 1998 en het daarop volgende *EU Data Protection Directive*, 1995. De lokale wetten verschillen echter aanzienlijk tussen de deelstaten, waardoor het voor bedrijven en overheden moeilijk is om grensoverschrijdend te werken als daar persoonlijke informatie mee is gemoeid.

De AVG verhelpt dit; het is één centraal uitgegeven wet die – zonder wijzigingen – effectief wordt in elk van de lidstaten, en zelfs daarbuiten als een niet-lidstaat persoonlijke informatie van EU-residenten verwerkt. Bijgevolg kunnen organisaties hetzelfde niveau van beveiliging verwachten in elk van de lidstaten als ook in staten buiten de EU voor zover het de bescherming van zulke data betreft.

Deze sterke vereenvoudiging zal de zakenwereld zo'n 2,3 miljard Euro op jaarbasis besparen, schatte de EU in haar Memo 17-1441.

Een ander nieuwtje is dat deze Regulation de boetes voor non-conformiteit en inbreuken vaststelt en niets meer te raden overlaat. De boetes zijn aanzienlijk en maken het overduidelijk dat de EU de bescherming van haar burgers uiterst serieus neemt.

Ook die rechten zet de AVG haarfijn uiteen zodat ook daarover geen misverstanden meer kunnen ontstaan. Het definieert bijvoorbeeld het *recht om vergeten te worden* en het recht om *voldoende te worden geïnformeerd* als er ongeoorloofde dingen met de data gebeuren.

1.3 Over 'persoonlijke informatie'

Tot de komst van de AVG kon een deelstaat zelf invulling geven aan de betekenis van de woorden 'persoonlijke informatie'. De Verordening geeft een eenduidige definitie – en gaat daarin veel verder dan de meeste lokale wetgeving deed.

Persoonlijke informatie omvat nu: *enige data waarmee een individu persoonlijk kan worden geïdentificeerd,* maar ook datatypes zoals IP-adressen die daartoe maar beperkt geschikt zijn. Naast 'harde' data zoals geboortedatum en beroep, omvat de term ook 'zachte' data zoals gezondheidsgegevens en informatie over de culturele achtergrond.

Zelfs als data is geanonimiseerd (of 'pseudo-anonimised'), valt ze onder de definitie als het mogelijk is om de data zodanig te bewerken dat de personen met een redelijke graad van zekerheid identificeerbaar zijn.

1.4 Op wie van toepassing?

Net als de eerdere Directives, onderscheidt ook de AVG de Data-*Verwerker* van de Data-*Verwerkingsverant-woordelijke;* beiden zijn onderworpen aan de Regulatie.

- De ***Verwerkingsverantwoordelijke*** is de verantwoordelijk voor het verwerken. Dit is bijvoorbeeld de klant van Combell die een online datingsite uitbaat en daartoe gegevens verwerkt zoals namen, persoonlijke voorkeuren en betaalgegevens. Om dit in goede banen te leiden, is de Verwerkings-verantwoordelijke verplicht om aan de *Verwerker* te melden hoe hij deze specifieke data moet verwerken – en zelfs *waarom*. De Verwerkingsverantwoordelijke moet ervoor instaan dat de verwerking wettig is, een specifiek (legaal) doel dient én transparant wordt uitgevoerd;
- De ***Verwerker*** is de entiteit die de data verwerkt zoals de Verwerkingsverantwoordelijke die aanlevert. Als Combell bijvoorbeeld de backup voor de klant in de voorgaande bullet beheert, zijn wij de Verwerker van die databewerking. Wij moeten dan logs bijhouden van die bewerking en zijn verantwoordelijk voor incidenten die aan Combell verwijtbaar zijn;
- De Verwerker moet er tevens voor zorgen dat ***enige derde partij*** die hij inhuurt in verband met de Verwerking, volledig conform de AVG werkt. Dergelijke partijen duidt de AVG aan met de term 'sub-Verwerkers' en de Verwerker is volledig verantwoordelijk voor inbreuken die volgen uit het inhuren van een sub-Verwerker.

De personen wiens persoonlijke informatie wordt verwerkt, duidt de Regulation aan als zijnde de 'data subjects' (of kortweg 'subjects').

*Note: de AVG is eveneens van toepassing op Verwerkers en (sub)-Verwerkers **buiten de EU** als de bewerking plaatsvindt op persoonlijke data van residenten van de EU.*

1.5 Wettige verwerking

Het eerste dat de Verwerkingsverantwoordelijke moet vaststellen, is of de verwerking wel wettig is. De AVG laat ook hier niets aan de verbeelding over en definieert de volgende gevallen als 'wettig' (er moet aan tenminste één van de criteria worden voldaan).

- ***Voldoen aan verplichtingen onder een overeenkomst*** – zeer relevant voor de relatie tussen een klant en Combell, is de situatie waarin wij de Verwerkingsverantwoordelijke zijn van de persoonlijke informatie van vertegenwoordigers van die klant. Het gaat daarbij vooral om contactgegevens van personen bij Accounts Payable en projectmanagers, technische contactpersonen, enzovoort;
- ***Actieve toestemming van het data subject*** – in plaats van slechts een 'opt-out' vakje *niet* aan te klikken of akkoord te gaan met Algemene Voorwaarden waarin tevens een opt-in is verstopt, moet het subject *actief toestemming geven* voor de verwerking. Deze toestemming moet bovendien deugdelijk worden opgeslagen – en moet eenvoudig weer kunnen worden ingetrokken. De verwerking is alleen geldig als aan al deze voorwaarden is voldaan;
- ***Wettelijke verplichting*** – alle verwerking die men doet om aan andere wetten te voldoen, is uiteraard ook wettig onder de AVG;
- ***Persoonlijke veiligheid / gezondheid*** – relevant in bijvoorbeeld de gezondheidszorg: persoonlijke informatie mag bewerkt worden als dit van essentieel belang is voor het leven van het subject;
- ***Algemeen belang*** – verwerking die het publieke belang dient, is eveneens wettig onder AVG;
- ***Legitiem belang van de Verwerkingsverantwoordelijke*** – de AVG staat ook verwerking toe als dit een legitiem belang van de Verwerkingsverantwoordelijke dient, zoals het kunnen identificeren van individuen die verantwoordelijk zijn voor hacking, fraude, enzovoort;
- ***Legitiem belang van derde partij*** – bijvoorbeeld een overheidsdienst die verwerking vereist in het kader van een crimineel onderzoek.

2 Een inbreuk – en nu?

2.1 Verwerkingsverantwoordelijke waarschuwt de autoriteiten

Afhankelijk van de aard van de gelekte data, bent u de Verwerkingsverantwoordelijke of de Verwerker. Aangezien u in de rol van *Verwerkingsverantwoordelijke* slechts 72 uur hebt om de *autoriteiten* te waarschuwen (op straffe van een forse boete), is het zinnig om ***op voorhand*** te evalueren voor welke datasets u de Verwerkingsverantwoordelijke bent!

Tip: organisaties met een Information Security Board en Security Officer, hebben zeer waarschijnlijk een Risk Assessment-mechanisme ingericht. Dit proces leent zich prima voor de genoemde evaluatie en haakt bovendien in op een Corrective Action-proces om eventuele problemen te corrigeren.

Bij twijfel, overlegt u *altijd* met ons over datasets die op een door Combell beheerd platform staan, zodat we samen kunnen vaststellen wie welke rol vervult – voordat zich een daadwerkelijk incident voordoet en we de 72 uren beginnen af te tellen.

2.2 De Verwerker waarschuwt de Verwerkingsverantwoordelijke

Als Combell uw Verwerker is en we menen dat er een inbreuk kan zijn geweest – zoals gedefinieerd onder Artikel 33 en 34 van de AVG -, informeren wij u, de Verwerkingsverantwoordelijke, op de kortst mogelijke termijn. Dit stelt u in staat om de passende autoriteiten te waarschuwen als dat wettelijk vereist is.

2.3 Waarschuw uw Data Protection Authority

2.3.1 Voorlopig rapport binnen 72 uur

De limiet van 72 uur maakt het moeilijk om een compleet rapport in te dienen; u als de Verwerkingsverantwoordelijke heeft dan waarschijnlijk nog niet alles boven tafel gekregen. De AVG onderkent dit en stelt dat uw *eerste* in ieder geval de volgende informatie moet bevatten:

- Het type inbreuk dat u vaststelde / vermoedt;
- Het aantal data subjects dat mogelijk een risico loopt;
- Het risico dat de inbreuk met zich meebrengt (voor de betrokken subjects);
- De maatregelen die u al had genomen ten tijde van uw melding;
- De maatregelen die u nog voornemens bent te gaan nemen.

2.3.2 Contactinformatie van uw Data Protection Authority

Voor België kunt u de website van de Belgische Privacy Commission gebruiken. Deze site is beschikbaar in het Nederlands, Frans en Engels.

Voor Nederland gebruikt u de online notificatie van de Autoriteit Persoonsgegevens. Het formulier is alleen in het Nederlands beschikbaar.

2.4 Melding van inbreuk aan data subjects

Een inbreuk is gedefinieerd als: *een schending van de beveiliging die ertoe leidt dat de data wordt…*

- Vernietigd,
- Verloren,
- Gewijzigd (verminkt),
- Ongeoorloofd wordt ontsloten,
- Ingezien door ongeautoriseerden.

De Verwerker is verplicht de Verwerkingsverantwoordelijke te helpen bij het opstellen van de notificatie aan de data subjects; het detailniveau waarop Combell gegevens zal aanleveren, hangt vooral af van de technologische en organisatorische maatregelen die deel uitmaken van het servicepakket dat onze klant (de Verwerker) afneemt.

3 Uzelf, als 'data subject' van Combell

Het volgende is van kracht als Combell uw persoonlijke data verwerkt. We houden bijvoorbeeld gegevens bij van personen met wie wij contact hebben om aan onze verplichtingen onder een Overeenkomst te kunnen voldoen (facturatiecontact, escalatiecontact voor Security Incidenten, technische contactpersonen, enzovoort).

3.1 Uw recht om vergeten te worden

Data subjects hebben het recht te vereisen dat de Verwerker hun data wist, als het doel waarvoor de data origineel werd verzameld, is vervallen. U kunt hetzelfde eisen als u uw toestemming intrekt, en/of een redelijk bezwaar aandraagt tegen de wijze waarop Combell de data verwerkt.

Het is onze verantwoordelijkheid om mogelijke onderaannemers die bij de serviceverlening betrokken zijn, te contacteren opdat zij ook kopieën van (of links naar) uw data verwijderen. Zulke partijen kunnen namelijk sub-Verwerker zijn en dan is het de verantwoordelijkheid van ons, als Verwerker, dat ook zij conform de AVG acteren.

3.2 Recht te weten welke data hoe wordt verwerkt

Personen hebben het recht te weten welke data we aanhouden; ook mogen zij correcties opdragen als de data incorrect of incompleet is. Verder mag een data subject ons om gerelateerde informatie vragen, zoals:

- De termijn waarover de informatie zal worden bewaard;
- Onze justificatie voor het bewerken;
- Welke personen / organisaties toegang hebben tot de informatie.

Afhankelijk van het type data, verstrekken we directe (beveiligde) toegang ertoe of leveren een direct kopie op in een industriestandaard formaat (bijvoorbeeld in het CSV-formaat).

Merkt u op dat data subjects deze informatie met 'redelijke intervallen' kunnen opvragen, hetgeen bijvoorbeeld inhoudt dat een contactpersoon voor facturen geen maandelijkse update mag vragen van gegevens zoals opgeslagen e-mailadres, naam en aanhef.

3.3 Recht op datamigratie

U hebt het recht uw data naar een andere Verwerker te verhuizen, in vrijwel de meeste gevallen zonder dat uw huidige Verwerker u daarvoor kosten zal aanrekenen. Combell zal bijvoorbeeld uw data in een industriestandaard formaat aanleveren (zoals in een CSV-bestand of een ander, dit afhankelijk van de situatie en uw voorkeuren) binnen één maand na uw verzoek daartoe.

4 Onze implementatie

4.1 Algemeen

Zoals de juridische lezer wellicht zal herkennen, zal de nieuwe 'General Data Protection Regulation' inzake de bescherming van persoonlijke informatie voor alle Europese lidstaten van kracht zijn vanaf mei 2018. Omdat conformiteit met deze wetgeving praktische implicaties met zich meebrengt, heeft Combell haar 'dataprivacy'-implementatie vroegtijdig ingezet.

De wijze van implementeren verzekert u en ons ervan dat Combell conform GDPR opereert. De belangrijkste onderdelen van het programma zijn deze:

- We richtten een separaat proces in voor inbreuken op (informatie)veiligheid;
- Voerden het verplichte declaratieproces reeds door;
- Hebben standaard een Data Processing addendum op onze Master Service Agreements beschikbaar;
- Blijven ons serviceportfolio uitbreiden met optionele beveiligingsdiensten;
- En analyseren onze interne processen om bescherming van privacy een *standaardonderdeel* van bestaande en nieuwe producten te maken.

Omdat we tevens marktleider zijn op het gebied van Managed Hosting in Nederland, hebben we conformiteit met de Nederlandse wetgeving ook al doorgevoerd. Bovendien hebben diverse van onze Belgische klanten bijkantoren in Nederland. Om aan hun specifieke eisen te kunnen voldoen, namen we ook alle maatregelen om conform de Nederlandse (progressieve) wetgeving te werken.

Het veilig bewerken van persoonlijke data is een van de belangrijkste vereisten van de GDPR; het omvat het voorzien van ***passende*** technologische en organisatorische maatregelen. Aangezien 'passend' geen sluitende definitie is, specifieert de GDPR dat deze maatregelen moeten worden gebaseerd op het type verwerking dat plaatsvindt.

- Combell biedt daarom standaard een set van essentiële maatregelen als vast onderdeel van onze diensten;
- Plus een *aanvullende* set van beveiligingsdiensten om een klant-specifieke oplossing verder toe te snijden op het beveiligingsniveau dat die klant vereist.

De beveiliging van het bewerken schept verplichtingen aan zowel de *Controller* als de *Processor* en het is dan ook van vitaal belang dat onze klanten ons informeren over hun datasets (aard, strekking en oogmerk) als wij een onderbouwd advies moeten uitbrengen.

4.2 Technische en organisatorische maatregelen

Combell biedt *standaard-* en *optionele, aanvullende maatregelen* om het gewenste niveau van (Informatie) Beveiliging te bereiken.

4.2.1 Standaardmaatregelen

Combell biedt het volgende, als vast onderdeel van haar diensten:

- Een Beveiligingspolicy voor medewerkers om de Information Assets te beschermen tegen diefstal, verminking, verlies, onbeschikbaarheid en onrechtmatige ontsluiting;
- Transparantie over de locatie en eigenschappen van onze Tier 3-conforme datacentra;
- Een strikt beleid om geen persoonlijke informatie buiten de EU te brengen zonder de uitdrukkelijke toestemming van de Controller;
- Serviceverlening onder Belgische, Nederlandse of Deense wetgeving, dit afhankelijk van de voorkeuren van de klant;
- Transparantie over onze sub-Processors en onderaannemers (we werken uitsluitend met zorgvuldig geselecteerde derde partijen);
- Regelmatige audits om conformiteit te verzekeren en het gewenste niveau van vertrouwen te bewerkstelligen tussen Combell en onze klanten:
    - Tenminste eenmaal per jaar auditen medewerkers van een bepaalde afdeling de maatregelen binnen een andere afdeling;
    - Een gecertificeerde externe auditor voert een onafhankelijk onderzoek uit (eveneens jaarlijks of vaker);
    - Ad-hoc audits vinden plaats op uitdrukkelijk verzoek van klanten;
- Een ISO 27001-gecertificeerd *Information Security Management System*, onderwerp van de genoemde audits. Ons Security Incident Management-proces verzekert klant én Combell er onder meer van dat wij tijdig zullen reageren nadat een datalek is vastgesteld;
- Strikte garanties als onderdeel van onze Service Level Agreements, die de beschikbaarheid verzekeren, ondersteund door praktische maatregelen zoals een regelmatig getest Business Continuity Plan;
- Complete scheiding van *verantwoordelijkheden* met twee gedefinieerde hoofdcategorieën, te weten de Office Zone en de Customer Zone:
    - Een manueel proces stelt zeker dat alléén medewerkers met de juiste autorisaties een Zone kunnen binnengaan;
    - Alle aanmeldingen worden gelogd en de uitkomsten veilig opgeslagen;
- Complete scheiding van *data:*
    - Klanten kunnen kiezen voor een *dedicated private* cloud of een shared *multi-tenant* cloud;

    - Een brede set technologieën voorkomt lekken tussen de gebruikers, bijvoorbeeld: VMware Encapsulation, beveiligde LUNs op de storage en virtuele LAN's (vLAN's) plus VPN's om het dataverkeer in transit te scheiden[1].
- Een Out-of-Production proces dat verzorgt dat de data zeker wordt verwijderd van dedicated Assemblies bij aflopen van het contract, als ook van *shared* Assemblies (zoals backupvoorzieningen) bij het aflopen van de retentieperiode;
- De dienst *Basic* DDOS Protection*, die verdacht verkeer 'afknijpt' en een alarm slaat. De meeste van dergelijke aanvallen slaan we al aan de buitenrand van onze backbone af zodat zij de gehoste omgevingen niet bereiken;
- Geoptimaliseerde OS & Application Logging, dat aanvullende audit- en loginformatie biedt voor Incidente Response en forensisch onderzoek. Dit stelt klanten in staat om rapporten op te stellen aangaande de scope van een breach, voor verdere interne en externe communicatie;
- OS Hardening Guidelines die zorgvuldig geselecteerde software en hun implementatie omschrijven. Dit minimaliseert de kans op nieuwe zwakheden in Assemblies en voorkomt de installatie van onnodige services die de beveiliging kunnen beïnvloeden;
- *Basic* Patch Management* voert in voorgedefiniëerde 'Patch Windows' de belangrijkste patches door op de door Combell beheerde besturingssystemen. Automatisering maakt dit proces kostenefficiënt en betrouwbaar.

**: Van deze Basic-services bestaat ook een Advanced versie als een optionele aanvullende service. Deze zijn nader omschreven in de volgende paragraaf.*

4.2.2 Optionele, aanvullende maatregelen

Klanten kunnen elk van de hierna genoemde servicecomponenten kiezen, voor zover de door hun geselecteerde services die natuurlijk ondersteunen.

- Managed Detection and Response: detecteert netwerk-gebaseerde aanvallen en biedt een praktische notificatiefunctie (gericht op *uw* organisatie en *uw* eigen ICT-platform), inclusief advies tot remediatie van onze Operations en Security Operations Centre;
- Maatwerkafspraken voor Recovery *Time,* Recovery *Point*, en *backup-retentietijden* om aan bijzondere beveiligingseisen te kunnen voldoen;
- Data Sanitisation Services om virtuele / fysieke storagevolumes te wissen, vernietigen of te overschrijven;
- *Advanced* DDoS Protection dat verkeer omleidt via een externe 'scrubbing service' zodat alleen het geschoonde verkeer bij de omgeving van onze klant terechtkomt;
- Managed Detection & Response, dat continu inzicht geeft in de IT-omgeving zodat klanten digitale bedreigingen en breaches kunnen detecteren. Ondersteund door het gerenommeerde Fox-IT en kundige analisten van de SOC- en Intelligence-teams, biedt deze dienst onze klant volledig inzicht én praktisch advies inzake remedies van ter zake kundig personeel;

[1] Vraagt u ons naar het aparte document, '*Information Security -versus- de Service Piramide*' en vermeld daarbij in welk type dienst u interesse heeft (shared of dedicated).

- Logaggregatie dat de logfiles centraal wegschrijft, buiten de Assemblies die de logs creëren. Dit verzekert u en ons ervan dat de logs juist zijn (*integer*) als ook *beschikbaar* en *confidentieel* blijven;
- *Advanced* Patch Management dat het door Combell beheerde OS bijwerkt met belangrijke patches, tijdens een Patch Window dat de klant heeft geselecteerd;
- Intrusion Detection & Protection Systems en anti-virus / anti-malwareservices, die de virtuele / fysieke Assemblies beschermen tegen bekende én onbekende zwakheden in webapplicaties, Enterprise-applicaties en besturingssystemen (‘zero day patching’);
- Web Application Firewall, dat publieke websites tegen de nieuwste bedreigingen beschermt op een kostenefficiënte wijze;
- Vulnerability Scanning, dat helpt om verborgen zwakheden te ontdekken voordat een aanvaller dat doet. Het identificeert systemen die moeten worden gepatcht – maar ook zwakheden die het systeem toegankelijk kunnen maken voor onbevoegden;
- SSL VPN met 2 Factor Authentication, dat een beveiligde tunnel over internet aanlegt tussen de lokale systemen van de klant en de gehoste systemen, via een webinterface.

5 Nawoord

5.1 Een 'work in progress'; uw mening is belangrijk

Dit document is een 'levend document' en Combell voegt er regelmatig onderwerpen aan toe.

Hebt u een versie van enkele maanden oud of wilt u bijvoorbeeld eenzelfde document inzake een *Private* Cloud-oplossing ontvangen, neemt u dan contact met ons op en we sturen u die documentatie toe. Een kort mailtje aan uw contactpersoon bij Combell of aan info@combell.com is al genoeg.

Alle feedback is zeer welkom! Combell doet er alles aan om helder te communiceren maar wellicht hebben we hier en daar de plank misgeslagen. We horen het heel graag van u als u ruimte voor verbetering of aanvullende informatie ziet.

5.2 Is dit uw eerste contact met ons?...

Is dit uw eerste contact met ons? Dan willen we graag nader met u overleggen inzake het inpassen van de hierin aangehaalde technologieën en methodieken in uw ICT-landschap.

Dat gesprek, zo hopen wij, zou weleens het begin kunnen zijn van een waardevolle 'Service Level e*X*perience'!

Alle zeilen bijzetten

"Als een klant op ongebruikelijk korte termijn een financieel voorstel moet krijgen, zie je dat het hele accountteam ***alle zeilen bijzet*** om het onmogelijke mogelijk te maken."

"Natuurlijk plannen we liefst alles netjes in, maar in de praktijk breekt nood vaak wet. Klanten waarderen ook hoe we zoveel mogelijk rekening houden met hun ***business***, in plaats van onze eigen ***afdelingsplanning***."

-- Fauve Hamerlynck
Internal Sales & Backoffice