progreso

HR software
MADE IN BELGIUM

Impact van de GDPR op HR en de verwerking in Progreso

Inhoudstabel

Wat is GDPR?

De GDPR is de nieuwe Europese privacywetgeving die op 25 mei 2018 van kracht wordt. De General Data Protection Regulation vervangt de huidige Belgische privacy-wetgeving. De GDPR, ook wel gekend als de Algemene Verordening Gegevensbescherming (AVG) voorziet in een betere bescherming van natuurlijke personen in zake de verwerking van persoonsgegevens.

Voornaamste wettelijke verplichtingen

De GDPR-wetgeving heeft impact op elk bedrijf dat data van werknemers, kandidaten, freelancers, contractors, stagiairs, interims, etc. verwerkt. Hieronder vindt u een opsomming van de voornaamste wettelijke verplichtingen:

• aantonen dat u de nodige maatregelen genomen hebt om persoonsgegevens op een doeltreffende manier te beschermen;

• in vele gevallen is uitdrukkelijke toestemming nodig om persoons-gegevens op te slaan en te verwerken;

• data protection impact assessments moeten standaard ingebouwd worden bij verwerkingen van persoonsgegevens die een hoog privacyrisico inhouden. Het privacyrisico is bijvoorbeeld hoog als u bijzondere persoonsgegevens (vb. ras, geloofsovertuiging of gezondheidsgegevens) verwerkt;

• op een begrijpelijke manier meedelen welke data u verzamelt, wat u ermee doet en hoe lang u ze bewaart;

• inbouwen van bijkomende rechten: zoals recht op inzage, recht om vergeten te worden, recht op het corrigeren van gegevens;

• op elk moment compliance kunnen aantonen, onder andere via een register van verwerkingsactiviteiten;

• datalekken binnen de 72 uur melden aan de Gegevensbeschermingsauthoriteit. In bepaalde gevallen moeten ook de betrokkenen worden ingelicht.

Wat houdt GDPR in voor HR?

Verwerking van persoonsgegevens

Als het om beveiliging van persoonsgegevens gaat, is de belangrijkste boodschap: neem passende technische en organisatorische maatregelen. Een van de basisbeginselen van de AVG is namelijk dat uw organisatie passende en organisatorische maatregelen moet nemen om het lekken van persoonsgegevens te voorkomen. De vrije vertaling is dat u persoonsgegevens op een zorgvuldige manier moet opslaan en verwerken. Dit raakt juist uw vakgebied, omdat u veel met persoonsgegevens van werknemers te maken heeft, en u die in een beschermde omgeving moet verwerken.

Daarnaast hebben werknemers, kandidaten, freelancers, contractors, stagiairs, interims, leveranciers en service providers het recht om te weten wat er met hun persoonlijke data gebeurt.

Om in regel te zijn, moet u ervoor zorgen dat het duidelijk is hoe u de persoonsgegevens zal verwerken en dat ze:

• enkel worden verzameld voor uitdrukkelijk omschreven doeleinden en bovendien relevant en beperkt zijn tot die doeleinden;

U mag enkel data opvragen die u echt nodig hebt om de carrière van uw werknemer te begeleiden. Voor alle andere data moet u expliciet toestemming krijgen.

• worden verwerkt op een rechtmatige manier;
U mag data enkel gebruiken voor het doel waarvoor ze gevraagd zijn. Zo is bijvoorbeeld het zonder toestemming opslaan van persoonlijke contactgegevens in een werfreserve met de nieuwe datawet niet langer toegestaan.

• niet langer worden bewaard dan nodig;
Onder de nieuwe regelgeving mag u gegevens niet langer bijhouden dan nodig. Dit betekent bijvoorbeeld dat gegevens van sollicitanten die niet weerhouden werden na het sluiten van de procedure moeten verwijderd worden. Ook gegevens van werknemers die het bedrijf verlaten mogen maar kort bijgehouden worden.

• op een veilige manier worden verwerkt. Het is van groot belang dat uw organisatie op verschillende gebieden investeert in de beveiliging van systemen. In de vorm van trainingen en opleiding over het informatieveiligheidsbeleid, maar ook goed doordachte beveiligingsprocedures horen erbij. Die procedures moeten vervolgens duidelijk zijn voor iedere persoon in de organisatie die met persoonsgegevens werkt. Of dat nu een werknemer is, een ingehuurd personeelslid of een externe gebruiker.

Hoe kan uw bedrijf de correcte verwerking bewijzen of verantwoorden?

Dat kan op verschillende manieren:

• inventariseer alle verwerkings-activiteiten

• toon aan dat u enkel die gegevens verwerkt die u echt nodig hebt;

• stel een 'privacy notice' op (een verklaring waarin uw bedrijf beschrijft hoe het de data verzamelt, gebruikt, bewaart, ...);

• ontwikkel een intern beleid om uw medewerkers te trainen en te sensibiliseren

• stel minstens een 'privacy'-verantwoordelijke aan, of een Functionaris voor Gegevens-bescherming (DPO);

• voer indien nodig een impact-analyse, of Gegevensbeschermings-effectbeoordeling uit;

• gebruik efficiënte beveiligings-procedures;

• ...

Wat doet Progreso rond GDPR?

De GDPR maakt een onderscheid tussen de verwerkingsverantwoordelijke en de verwerker. De verwerkings-verantwoordelijke zegt hoe en waarom de persoonsgegevens worden verwerkt. De verwerker treedt op ten behoeve van de verwerkings-verantwoordelijke. Progreso verwerkt als verwerker data in opdracht van haar klanten. De gegevens van de eigen medewerkers verwerkt het als verwerkingsverantwoordelijke.

Zowel de verwerkingsverantwoordelijke als de verwerker moeten voldoen aan de nieuwe GDPR en hun 'daden' en processen kunnen verantwoorden, ze moeten met andere woorden allebei kunnen bewijzen of verantwoorden hoe die verwerking gebeurt en waarom.

Progreso voorziet voor de verwerking van de data van haar klanten in volgende items:

Verwerkersovereenkomst

In onze licentiecontracten is reeds opgenomen dat we uw gegevens verwerken en bewaren in overeenstemming met de Europese en Belgische regelgeving. In het kader van de GDPR/AVG verduidelijken we deze contractuele uitvoering verder in onze verwerkersovereenkomst.

Op grond van de GDPR moeten verwerkingsverantwoordelijken die gebruik maken van externe verwerkers – zoals onze klanten die gebruik maken van onze private cloud – een overeenkomst sluiten met de verwerker waarin zij aandacht besteden aan een aantal voor de juiste toepassing van de GDPR relevante onderwerpen. In art. 28 van de GDPR worden aan deze overeenkomsten een aantal eisen gesteld. De overeenkomst:

- benoemt het doel van de verwerking en verbiedt de verwerking van de gegevens voor een ander doel

- verplicht het vertrouwelijk houden (geheimhouding) van de gegevens door de verwerker en zijn medewerkers en door hem ingeschakelde andere verwerkers;

- verplicht de verwerker alle in art. 32 van de GDPR genoemde maatregelen te nemen. Deze maatregelen slaan op de beveiliging van de persoonsgegevens. Aansluiting bij een erkende gedragscode of certificering is ook mogelijk. Progreso doorloopt hiertoe sedert 2017 een traject voor een ISO/IEC 27001 certificering (informatiebeveiliging);

• regelt de verplichting van de verwerker om niet zonder toestemming van de verwerkingsverantwoordelijke een andere verwerker in te schakelen. Als de toestemming al vooraf is gegeven (algemene toestemming) dan wordt de verwerker verplicht de verwerkingsverantwoordelijke van zijn voornemen op de hoogte te brengen met vermelding van de omstandigheden die tot zijn keuze een andere verwerker in te schakelen hebben geleid. In alle gevallen is de verwerker verplicht om de door hem ingeschakelde verwerker te binden aan alle bepalingen uit de overeenkomst tussen hem en de verwerkingsverantwoordelijke;

• verplicht de verwerker om de verwerkingsverantwoordelijke behulpzaam te zijn bij verzoeken van de betrokkene op grond van hoofdstuk III van de GDPR, zoals bijvoorbeeld vergeet- of rechtzettingsverzoeken;

• regelt de verplichting van de verwerker om de verwerkingsverantwoordelijke bij te staan bij het uitvoeren van zijn verplichtingen die samenhangen met de bijzondere eisen met betrekking tot gegevensbescherming, zoals bijvoorbeeld het melden van datalekken en het uitvoeren van een zogeheten 'gegevensbeschermingseffectbeoordeling'.

• regelt wat er gebeurt aan het einde van de overeenkomst: worden gegevens gewist of teruggegeven;

• verplicht de verwerker om volledige medewerking te verlenen aan audits, inspecties en onderzoeken door of namens de verwerkingsverantwoordelijke.

Bijhouden van register van verwerkingsactiviteiten

Overeenkomstig de GDPR moet elke onderneming die "niet incidenteel" persoonsgegevens verwerkt hiervan een register bijhouden. In haar recente aanbeveling verduidelijkt de Privacycommissie dat ook personeelsbeheer als "niet incidentele" verwerkingen moeten worden beschouwd.

Deze verwerking geniet vandaag nog van een uitzondering op de aangifteplicht bij de Privacycommissie, maar zal vanaf de inwerkingtreding van de GDPR dus wel moeten worden opgenomen in een register.

Progreso houdt voor de verwerking van de personeelsgegevens van haar klanten een register bij van deze verwerkingen.

Een veilige verwerking

Risicogebaseerde aanpak

In het kader van de risico-gebaseerde aanpak voert Progreso voor alle informatiemiddelen een risicoanalyse uit op vlak van informatieveiligheid en privacy, om zo de beschermingsmaatregelen te maximaliseren.

Opleiding van medewerkers

Progreso waakt constant over de kwaliteit en dataprivacy in de aangeboden dienstverlening. Medewerkers worden op regelmatige basis in individuele en gezamenlijke teammeetings hieromtrent gebriefd.

Tweewekelijks organiseren we kwaliteitsoverleg waarin alle onderwerpen van de voorbije periode opnieuw worden overlopen. Hierin komen zowel mogelijke kwaliteitsissues als veiligheidsissues aan bod.

Informatieveiligheidsbeleid en procedures

Progreso is op de hoogte van haar verplichtingen in het kader van GDPR; er is een data privacy programma dat constant wordt gemonitord door onze Systems en security manager. Procedures zijn opgesteld voor de monitoring van alle security issues, waaronder een procedure voor het melden van datalekken.

De klantdata wordt bijgehouden op een private cloud, gehost in België. Medewerkers krijgen slechts toegang tot specifieke data op basis van rechten die door de Systems en security manager worden opgevolgd. Toegangen naar de applicatie zijn ge-encrypteerd.

Disclaimers en privacy notices

HR dient zorg te dragen voor intern beleid om persoonsgegevens te beschermen en toegang te hebben tot deze informatie. Hiertoe dient u medewerkers uitgebreid en in begrijpelijke taal te Informeren (vb bij de indiensttreding) over de verwerking van zijn/haar gegevens en hun daarbij behorende rechten.

Progreso voorziet in een nieuwe functionaliteit waarmee u voor elke rol in de applicatie (medewerker, trainer, kandidaten, HR,..) een disclaimer kan instellen die bij het inloggen dient aanvaard te worden. Indien wijzigingen aan deze disclaimer noodzakelijk zijn kan u deze resetten en opnieuw laten bevestigen door uw medewerkers

Anonimiseren of verwijderen van gegevens

Gegevens mogen enkel bewaard worden zolang dat nodig is om het oorspronkelijke doel te vervullen, bijvoorbeeld zolang een kandidaat in een selectieprocedure zit. U dient op voorhand duidelijk te definiëren hoe lang u de gegevens nodig hebt.

Progreso zal aan de hand van de termijnen die u ons bezorgt de gegevens van medewerkers en kandidaten onherkenbaar maken of verwijderen (anonimiseren of verwijderen).

Bij het onherkenbaar maken van gegevens bestaan er 3 mogelijkheden:

Pseudonimiseren

Bij pseudonimisering zorgt u ervoor dat de persoonsgegevens niet meer aan een specifiek persoon kunnen worden gekoppeld. Die link kan eventueel wel worden gelegd met aanvullende gegevens. Daarom moeten deze aanvullende gegevens apart worden bewaard. Een voorbeeld is het coderen van de laatste paar cijfers en letters van een paspoortnummer. De sleutel tot het terugtoveren van het complete paspoortnummer bewaart u dan in een andere database. Aangezien in het kader van GDPR een verplichting kan bestaan tot het permanent onherkenbaar maken van gegevens ondersteunt Progreso deze methode niet.

Anonimiseren

Anonimiseren is niet hetzelfde als pseudonimiseren: bij anonimiseren overschrijven we de gegevens die herleid kunnen worden naar een persoon en kunnen we deze niet meer terughalen. Denk aan alle geboortedata van werknemers in het systeem op 01-01-01 zetten of de achternamen van alle mensen in een bestand wijzigen in “MedewerkerX”.

Door anonimisering kunnen we wel detaildata blijven hanteren voor rapporteringsdoeleinden (vb rapport sociale balans) zonder dat privatieve gegevens van de medewerker zichtbaar zijn. Bij anonimiseren zullen tevens teksten waaruit de werknemer zou kunnen worden herkend worden overschreven, vb. commentaren in evaluatie- of functioneringsgesprekken.

Permanent verwijderen

Permanent verwijderen betekent het definitief verwijderen van een kandidaat of medewerker uit de database zonder de mogelijkheid om deze te restoren. Dit betekent dat op alle gerelateerde data van deze persoon (vb opleidingsgegevens, prestatiehistoriek,..) niet meer kan worden gerapporteerd aangezien deze definitief uit het systeem zijn geschrapt.

Exporteren van data van medewerkers en kandidaten

Dankzij de GDPR krijgen de betrokkenen veel meer rechten in verband met de verwerking van hun persoonsgegevens. Zo krijgen uw medewerkers, naast het reeds bestaande recht tot inzage in het personeelsdossier, het recht tot ontvangst van een kopie van het dossier

Progreso voorziet hiertoe voor HR in een mogelijkheid om het volledige dossier van een medewerker of kandidaat te exporteren naar een leesbaar formaat.