HR2day

dedicated HR software

Whitepaper AVG / GDPR

Versie 1.3 7 mei 2018

Inleiding

Vanaf 25 mei 2018 wordt in Nederland de Algemene Verordening Gegevensbescherming (AVG) van kracht en geldt in de gehele Europese Unie dezelfde privacywetgeving General Data Protection Regulation (GDPR). De verordening is gericht op een betere bescherming van persoonsgegevens en staat boven de landelijke wetgeving.

Het doel van de verordening is de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. Daarbij krijgen natuurlijke personen een aantal rechten waar jij wanneer je persoonsgegevens verwerkt aan moet kunnen voldoen.

De belangrijkste rechten waar je aan moet kunnen voldoen zijn:

- **Recht op informatie**
  Je moet kunnen aangeven welke gegevens en met welk doel je registreert (dataregister)
- **Recht op inzage**
  Je moet personen die daarom vragen inzage kunnen geven in de geregistreerde gegevens
- **Recht op correctie en verwijdering**
  De geregistreerde gegevens moeten kunnen worden aangepast of zelfs verwijderd als de persoon in kwestie daarom vraagt
- **Mogelijkheid om een klacht in te dienen**
  Je moet een meldingsprocedure hebben, waar mensen een klacht kunnen indienen als gegevens onterecht worden vastgelegd of openbaar worden gemaakt.

Omdat je als klant van HR2day persoonsgegevens vastlegt van medewerkers (en mogelijk ook van externen), leggen we in deze Whitepaper uit welke gevolgen de AVG met name heeft en hoe we samen kunnen zorgen dat je aan de AVG voldoet.

De belangrijkste gevolgen van de AVG

Feitelijk verandert er niet heel veel, immers de AVG is al in 2016 in werking getreden, maar vanaf 25 mei 2018 zal er worden gehandhaafd. Je zult dan moeten kunnen aantonen dat je voldoet aan de eisen die de AVG aan je stelt. Daarbij is het van belang dat je kunt aantonen dat HR2day voldoende technische en organisatorische maatregelen heeft getroffen om het beveiligingsniveau te waarborgen

Verwerkersovereenkomst

In de AVG wordt voorgeschreven dat organisaties die andere partijen inschakelen om persoonsgegevens te verwerken, met deze partijen een verwerkersovereenkomst moeten afsluiten. Met een verwerkersovereenkomst sluit je uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken. HR2day heeft een standaard verwerkersovereenkomst opgesteld die aan alle klanten ter ondertekening is aangeboden. In deze overeenkomst leggen we de wederzijdse rechten en plichten vast. De verwerkersovereenkomst kun je vinden op: https://www.hr2day.com/verwerkersovereenkomst

Aantoonbaar veilige verwerking

HR2day is ontwikkeld en wordt uitgevoerd op het Salesforce platform. Gegevens van Europese organisaties worden opgeslagen in Europese datacenters. Als verantwoordelijke kun je aantonen dat de verwerking veilig is en voldoet aan de AVG/GDPR omdat:

- Medewerkers van HR2day verwerken geen gegevens, anders dan na toestemming door de opdrachtgever. De wijze waarop wij deze verwerking doen is ISAE3402 Type-2 gecertificeerd en de verwerking is onderhevig aan de overeengekomen Verwerkersovereenkomst. We verstrekken je dit ISAE-rapport jaarlijks op verzoek.
- Het Salesforce platform is ISO 27001 gecertificeerd, waardoor gegevens aantoonbaar veilig worden opgeslagen en verwerkt.
- Het Ministerie van Veiligheid en Justitie heeft in maart 2016 een vergunning afgegeven aan Salesforce voor de doorgifte van persoonsgegevens.
- Bij ministerieel besluit van januari 2017 is deze vergunning ook van toepassing op HR2day.

Functionaris Gegevensbescherming

HR2day heeft een Functionaris Gegevensbescherming (FG) aangesteld die ook is aangemeld bij de Autoriteit Persoonsgegevens. Deze FG houdt bij ons intern toezicht op de toepassing en naleving van de AVG en is je eerste contactpersoon in het (onwaarschijnlijke) geval van een datalek.

Verwijderen van (persoonsgegevens op) back-ups en na afloop contract

Eén van de meest lastige eisen in de AVG betreft het verwijderen van gegevens van personen die daarom vragen. Hierbij dient transparantie te worden gegeven over de persoonsgegevens in back-ups. Back-ups zijn benodigd om te kunnen voldoen aan continuïteitseisen en het voorkómen van een datalek als gevolg van verlies van persoonsgegevens. Daarom maken we onderscheid tussen het verwijderen van back-ups tijdens de contractperiode en na afloop van de contractperiode.

- **Tijdens de contractperiode** worden back-ups gemaakt om de continuïteit van de verwerking te garanderen. Dat betekent dat op een oudere back-up nog steeds persoonsgegevens kunnen staan, die inmiddels op verzoek zijn verwijderd. Verantwoordelijke (klant) dient in zo'n situatie na een eventuele recovery een procedure in gang te zetten om de data te verwijderen vanaf de back-up datum (zie ook de adviezen onder 'Recht om vergeten te worden'). De beschikbaarheid en toegankelijkheid van de gegevens op deze back-up vallen onder alle privacymaatregelen, zoals bij de normale verwerking.
- **Na afloop van de contractperiode** worden alle gegevens van onze klanten geschoond. Je hebt nog een periode van 30 dagen om mogelijke gegevens alsnog op te vragen. Daarna worden binnen 90 dagen alle persoonsgegevens verwijderd. Ook de gegevens op de back-ups worden daarna binnen 180 dagen allemaal geschoond. Schijven en ander materiaal dat niet wordt hergebruikt wordt eerst volledig geschoond voordat het buiten gebruik wordt genomen. Ook deze processen vallen onder onze veiligheids- en privacymaatregelen.

Hoe zorgen we samen dat jij aan de AVG voldoet?

De Autoriteit Persoonsgegevens (AP) heeft een heel handig 10-stappenplan. Je vindt dit stappenplan op de website van de AP:
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg

De belangrijkste zaken die je moet regelen hebben wij vast voor je in kaart gebracht. Met daarbij de maatregelen die wij hebben getroffen zodat jij aan de AVG kunt voldoen. De zaken waar we samen aan kunnen werken zijn:

Stel een dataregister op

Een dataregister of register van verwerkingsactiviteiten is een overzicht van alle gegevens die je vastlegt, met een vertrouwelijkheidsclassificatie, de doelstelling van vastlegging, waar ze worden opgeslagen, welke functionarissen hier toegang toe hebben en eventuele derden die deze gegevens ontvangen. Je moet daarbij ook in kaart brengen welke risico's aan de registratie kleven.

HR2day bevat een hulpmiddel waarmee je op eenvoudige wijze een overzicht met alle objecten en velden kan oproepen. Hierin kan je de objecten en velden die je niet in gebruik hebt uitfilteren en relevante kenmerken zoals classificatie en redenen van registratie toevoegen.

Denk goed na over de autorisatie: privacy by default & privacy by design

Als organisatie blijf je zelf verantwoordelijk wie, waar welke gegevens mag verwerken. Zorg dus dat je vooraf goed nadenkt welke functionaris welke gegevens nodig heeft. En bedenk ook dat jij verantwoordelijk bent voor alle gegevens die binnen jouw organisatie worden vastgelegd. De velden in HR2day dienen een bepaald doel, te herkennen aan naam en helpteksten. Bij bijzondere of gevoelige gegevens ondersteunen we dat vaak met controles en/of standaard keuzelijsten. Maar je kunt vrije velden misbruiken door er andere gegevens in te vullen dan waarvoor het veld bedoeld is. Controleer hier regelmatig op, bijvoorbeeld door de uitgebreide (controle) rapportages die we bieden.

HR2day houdt bij de ontwikkeling van (nieuwe) functionaliteit standaard rekening met privacy. Gegevens worden eenmalig aan de bron vastgelegd en de autorisatie wordt maar eenmalig ingericht voor alle functionaliteit. Toegang tot (persoons)gegevens in HR2day wordt geregeld door het inrichten van profielen, rollen en scherminstellingen. Daarmee zorg je ervoor dat gebruikers toegang hebben tot de gegevens passend bij hun functieprofiel. Managers krijgen minder gegevens te zien dan administrateurs of beheerders. Met de rollen wordt de toegang automatisch beperkt tot die medewerkers waar de gebruiker op basis van de rol in de organisatie recht op zou moeten hebben.

Gebruik van gegevens

Niet iedere gebruiker mag zomaar alle persoonsgegevens van een ander zien. Het gebruik moet overeenkomstig het doel zijn. Niet alle gebruikers mogen bijvoorbeeld zomaar het BSN-nummer van een medewerker zien. We beoordelen alle functionaliteit en persoonsgegevens van HR2day. Een belangrijk aspect daarbij is de scheiding van gegevens op de schermen. We inventariseren alle schermen in HR2day en beoordelen of de persoonsgegevens die er staan in overeenstemming zijn met het doel.

Op basis van die inventarisatie zullen we sommige velden verbergen of verplaatsen zodat ze alleen voor de juiste geautoriseerden zichtbaar zijn.

Zorg dat medewerkers gegevens kunnen inzien, corrigeren en verwijderen

Medewerkers hebben via het Employee Interaction Center toegang tot al hun persoonlijke gegevens. Als je workflowprocessen hebt ingericht kan de medewerker ook eenvoudig een wijziging in die gegevens aanvragen.

Ook salarisspecificaties kan de medewerker inzien in het Interaction Center. De medewerker kan er voor kiezen deze ook per email te laten toesturen. We wijzen je erop dat dit (afhankelijk van de instellingen bij het privé emailaccount) minder veilig kan zijn. Daarom kan de werkgever deze mogelijkheid ook uitzetten.

Een beheerder heeft toegang tot alle gegevens. Hij kan eenvoudig met behulp van een aantal rapporten alle gegevens van een medewerker oproepen in Excel. Als een medewerker een gegeven wil laten wijzigen dat geen onderdeel is van een workflowproces kan de beheerder dat voor hem doen. De beheerder kan op verzoek ook gegevens verwijderen.

Recht om vergeten te worden

Medewerkers hebben het recht je te vragen 'vergeten te worden' uit de systemen. Je moet hier gevolg aan geven voor zover dat niet strijdig is met je wettelijke verplichtingen. Bij het opvolgen van een dergelijk verzoek is het volgende van belang:

- Zorg dat alle verzoeken worden geregistreerd.
- Indien het verzoek gerechtvaardigd is, verwijder je de gegevens in HR2day.
- De persoonsgegevens zijn dan nog aanwezig in back-ups (zie ook de toelichting hierboven). Indien een back-up teruggezet moet worden, moet je er voor zorgen dat de verwijderingen nogmaals worden uitgevoerd.

De mogelijkheid om medewerkergegevens te verwijderen bieden we in HR2day al langer. Daarvoor bieden we verschillende mogelijkheden, die we de komende periode verder zullen uitbreiden:

- **Verwijderen van persoonsgegevens** (medewerker, beoordelingen, documenten, etc) heeft altijd al bestaan in HR2day. Verwijderen is ook echt verwijderen. Eenmaal verwijderde gegevens kunnen nog gedurende 15 dagen door de systeembeheerder worden teruggehaald, maar daarna zijn ze echt weg. Mocht je een sandbox hebben of een pro-forma werkgever, verwijder de gegevens dan ook in die omgevingen. Houdt hier wel rekening met de wettelijke beperkingen die je hebt in verband met het voeren van een salarisadministratie.
- Onderzoek naar **anonimiseren van persoonsgegevens**. We zijn een onderzoek gestart naar het automatisch kunnen anonimiseren van persoonsgegevens voor archiveringsdoeleinden.

Vraag en registreer toestemming

De AVG stelt strenge eisen aan de toestemming die natuurlijke personen moeten geven. Bij medewerkers vraag je deze toestemming vaak al in de arbeidsovereenkomst, maar ook bij externen dien je deze toestemming expliciet te vragen. Zorg dat je aan kunt tonen dat je een geldige toestemming hebt verkregen.

Via de workflows van HR2day kun je het vragen en registreren van toestemming eenvoudig vastleggen in het personeelsdossier van de medewerker. Bij bepaalde functionaliteit (bijvoorbeeld portfolio) hebben we deze toestemming expliciet in de functionaliteit opgenomen zodat medewerkers zelf kunnen bepalen welke gegevens ze met anderen willen delen.

Dataportabiliteit

Een van de eisen die de AVG stelt is dat je persoonsgegevens moet kunnen exporteren zodat je deze in andere situaties weer kunt gebruiken. De huidige mogelijkheden die HR2day biedt, zoals het downloaden van gegevens in XLS of het versturen via een koppeling, zijn voldoende om aan de wet te voldoen.

Zorg voor een veilige toegang: 2-factor authenticatie

In de Algemene Verordening Persoonsgegevens (AVG) wordt het gebruiken van 2-factor authenticatie bij toegang tot persoonsgegevens ten zeerste aangeraden. Hierbij wordt de identiteit van de gebruiker getoetst op basis van twee 'factoren':

- Iets wat de gebruiker weet, zoals een wachtwoord
- Iets wat de gebruiker heeft, zoals een mobiele telefoon

Als je gebruik maakt van Single Sign-on (SSO) wordt de toegang tot HR2day automatisch gekoppeld aan de inlog in bijvoorbeeld je intranet of bedrijfsnetwerk: als je je daarbij hebt aangemeld kan je zonder aanvullende handelingen met één druk op de knop inloggen in HR2day. Hou er rekening mee dat de het authenticatieniveau dan dus ook door de SSO-oplossing wordt bepaald.

Bij rechtstreeks inloggen in HR2day heb je altijd een vorm van 2-factor authenticatie: naast het invoeren van de gebruikersnaam en wachtwoord moet je bij inloggen op een nieuw apparaat of vanuit een nieuw IP-adres een code overnemen die je ontvangt in je mail.

Je kan ook gebruik maken van de Salesforce Authenticator App. Met deze App bevestig je je identiteit telkens als je inlogt in HR2day met je vingerafdruk of een pincode. Dit wordt gezien als een zwaardere vorm van 2-factor authenticatie dan de standaardvorm met een eenmalige bevestigingsmail.

HR2day

dedicated HR software

Built on the world's #1 platform Salesforce

www.hr2day.com