Wolters Kluwer

GDPR PRODUCTFICHE

Verifield RiskReporter

1. **Aard van de Verwerking**
   Software om de risico's inherent aan een veiligheids- en milieubeleid te beheren en op te volgen via action management.

2. **Categorieën van Persoonsgegevens die verwerkt worden**
   Verwerker zal uitsluitend volgende categorieën van Persoonsgegevens verwerken in het kader van dit Addendum:

   ☒ identiteitsgegevens (naam, adres, gsm, e-mail, geboortedatum, nummerplaat, IP-adres, …)
   ☒ contactinformatie (adres, e-mail, IP-adres, IMEI, …)
   ☒ sociale status (functie op het werk, maatschappelijke functie, gezinssituatie, …)
   ☒ werkgegevens (beoordelingen)
   ☒ gedragsgegevens (surfgedrag, betalingsgedrag, gebruikshistoriek, …)

3. **Categorieën van Betrokkenen**
   ☒ eigen klanten van de Verwerker
   ☒ eigen werknemers Verantwoordelijke

4. **Doeleinden van de verwerking**
   ☒ levering van goederen of diensten
   ☒ business analytics

5. **Retentieperiode**
   Persoonsgegevens zullen verwerkt en bijgehouden worden gedurende volgende periodes:

   Ingevoerde Persoonsgegevens: worden onmiddellijk gewist en/of vernietigd na einde van de Overeenkomst

   Persoonsgegevens via helpdesk support: tot 3 maanden na einde van de Overeenkomst

6. **Beveiligingsmaatregelen**

   Technische en organisatorische maatregelen kunnen worden beschouwd als de stand der techniek op het moment van sluiten van de Overeenkomst van Dienstverlening. Verwerker zal technische en organisatorische maatregelen na verloop van tijd evalueren, daarbij rekening houdend met kosten voor doorvoering, aard, omvang, context en doelstellingen van verwerking, en het risico van verschillen in de mate van waarschijnlijkheid en ernst voor de rechten en vrijheden van natuurlijke personen.

Gedetailleerde technische en organisatorische maatregelen:	
Toegangscontrole: gebouwen	Toegang tot de gebouwen van Wolters Kluwer wordt door zowel technische als organisatorische maatregelen gecontroleerd: toegangscontrole met gepersonaliseerde badges, elektronische vergrendeling van deuren, receptieprocedures voor bezoekers.
Toegangscontrole: systemen	Toegang tot netwerken, operationele systemen, user administratie en applicaties vereisten de nodige autorisaties: geavanceerde paswoord procedures, automatische time-out en blokkering bij foutieve paswoorden,

	individuele accounts met historieken, encryptie, hardware en software firewalls.
Toegangscontrole: gegevens	Toegang tot gegevens zelf wordt beheerst door organisatorische maatregelen: user administratie en user accounts met specifieke toegang, opgeleid personeel omtrent gegevensverwerking en veiligheid, scheiding van de operationele systemen en de testomgevingen, toekennen van specifieke rechten en bijhouden van historieken van gebruik, toegang en wissing.
Encryptie van gegevens:	in transit en in rust
Vermogen om blijvende vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van verwerkingssystemen en -diensten te garanderen:	scheiding van productie- en testomgeving, scheiding van specifieke gevoelige gegevens, automatische back-up, geavanceerde paswoordprocedures, specifieke gebruiksrechten, bijhouden van historiek)
Vermogen om de beschikbaarheid van en toegang tot de Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident:	Back ups worden gemaakt in data center. Bij onderbreking heropstart binnen de 3 werkuren
Beschikbare certificering:	ISO/IEC 27001 certification

7. Subverwerkers

Wolters Kluwer laat geen gegevens verwerken door Subverwerkers voor deze applicatie.

8. Doorgifte van persoonsgegevens

Er vindt geen doorgifte van de persoonsgegevens plaats.