VERKLARING VAN OVEREENSTEMMING

Volgens de privacywetgeving (Wbp-NL en WVP-BE) moet iedere organisatie maatregelen treffen ter voorkoming van het onrechtmatig verwerken van privacy- en persoonsgevoelige informatie. Bedrijven en organisaties (de verantwoordelijke) zijn hierdoor verplicht om passende, preventieve en organisatorische maatregelen te nemen om aan de complexe privacywetgeving te kunnen voldoen. Daarnaast worden aanvullende eisen gesteld aan reglementen, overeenkomsten, procedures en methodes.

YourSafetynet ondersteunt de verantwoordelijke (per saldo de bestuurder van een organisatie) bij de uitvoering van de passende, preventieve en organisatorische maatregelen inzake Privacy- en ICT gebruiksbeleid. Via digitale wizards wordt de verantwoordelijke (of veiligheidsfunctionaris) stap voor stap door dit proces geleid. De inhoud van de ter beschikking gestelde procedures, templates, voorbeeldreglementen en overeenkomsten is in lijn met de privacywetgeving zoals die per 1 januari 2016 geldt. Na het voltooien van deze stappen, het correcte gebruik van de beschikbaar gestelde documenten en de correcte uitvoering van de geldende verplichtingen voldoet de organisatie aan de wettelijke eisen inzake de geldende privacywetgeving.

Wet- en regelgeving

- Documenten, procedures, reglementen en methodes
- Publicatie en distributie beleid op een voor iedereen toegankelijke wijze
- Integratieprocedures naar de organisatie, medewerkers, ondernemingsraad (OR) en/of alternatief overlegorgaan

Privacybeleid

- Wizard uitvoering privacybeleid
- Medewerkerovereenkomst intern privacy- en ICT beheer
- Reglement functionaris intern privacy- en ICT beheer
- Bewerkersovereenkomst extern privacy- en ICT beheer
- Vrijwaringsovereenkomst extern privacy- en ICT beheer
- Registratie toegangsrechten externe bewerkers (risico analyse)
- Procedure melding datalekken
- Formulier verwijdering inlogaccount
- Registratie intern gebruik persoonsgegevens (risico analyse)
- Registratie en opgave externe bewerkers
- Privacyreglement medewerkers
- Toestemming publicatie beeldmateriaal medewerkers

ICT Gebruiksbeleid

- Wizard invoering ICT gebruiksbeleid medewerkers
- ICT gebruiksreglement medewerkers
- Reglement BYOD gebruik medewerkers
- Reglement sociale media medewerkers
- Interne mededeling ICT gebruik binnen de organisatie

Technische implementatie en uitvoering

- Alle componenten van YourSafetynet (server, virtuele gateway en endpoint clients) communiceren onderling via beveiligde HTTPS verbindingen.
- Beveiligd technisch beheer voor (veiligheids)functionaris/ systeembeheerder. Uitsluitend via een HTTPS beveiligde web interface krijgt de functionaris toegang voor het beheer van alle instellingen, logs, statistieken en rapporten.
- De controle, rapportage en het beheer van internet- en computer op individuele personen is uitsluitend onder bepaalde condities toegestaan. De rapportage- en verwerkingsstatistieken worden in beginsel geanonimiseerd uitgevoerd.
- Optie tot selectieve en individuele maatwerkrapportage; na het toestaan van individuele selectieve controle worden geen andere gebruikers gerapporteerd.
- Vaststelling bewaartermijn verwerkte gegevens; hiermee kan de wettelijke bewaartermijn van gegevens worden ingesteld.
- Automatische vernietiging verwerkte gegevens; volgen van de weggooiplicht indien maximale bewaartermijn wordt overschreden.
- Toegepaste filtermethodieken; bijvoorbeeld als iemand zoekt op het woord 'borstkanker' dan mag dat absoluut geen sporen in de rapportage achterlaten.
- Interactieve controle op overtreding privacywetgeving; waarschuwingspop-ups verschijnen wanneer instellingen worden gemaakt die in strijd met de privacywetgeving.
- Online beschikbaarheid van individueel ingesteld privacy- en ICT gebruiksbeleid; via de YourSafetynet client zijn deze beleidsdocumenten (opnieuw) opvraagbaar.