Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

Informatiebeveiligingsbeleid (IBB)

De veiligheid van de software die Competentie Thermometer BV (hierna: CT) aanbiedt, staat hoog in het vaandel. We hebben daarom een Informatiebeveiligingsbeleid (IBB) met procedures en protocollen opgesteld. Op deze manier is zowel intern als voor voor klanten helder hoe gehandeld dient te worden in verschillende situaties. Het IBB is een formeel beleidsdocument dat tweemaal per jaar wordt herzien en aangevuld.

Leeswijzer

Dit document is de basis van een set documenten met betrekking tot veiligheid en privacy.
Algemene Voorwaarden – De voorwaarden van CT waarmee klanten akkoord gaan bij het aangaan van de Overeenkomst voor het gebruik van de software;

- **Calamiteitenplan** – Intern document met beleid en beschrijving van de procedures bij diverse calamiteiten zoals een storing, diefstal, datalek, nalatigheid of uitval;
- **Privacyverklaring** – Beschrijving van de omgang met gegevens en gevoelige informatie van klanten, waarin tevens wordt aangegeven welke gegevens worden verwerkt bij bezoekers van de website en social media;
- **Procedure Datalek** – Beschrijving van de procedure in het geval van een datalek waarbij gevoelige informatie van klanten door derden kan worden ingezien of gebruikt. De wet Melding Datalek vereist dat iedere organisatie een procedure heeft opgesteld in het geval van een datalek;
- **Risico Instructie** – Instructie voor medewerkers en partners van CT met beschrijving van mogelijke gevaren en risico's van het werken met gevoelige gegevens en een beschrijving van de verantwoordelijkheden, functies en taken van de verschillende personen binnen de organisatie;
- **Verwerkersovereenkomst** – Overeenkomst die wettelijk gezien door de klanten van CT in de rol van Verwerkingsverantwoordelijke, met CT in de rol van Verwerker moet worden afgesloten op basis van de Algemene Verordening Gegevensbescherming. CT heeft hier een modelovereenkomst voor opgesteld die wordt voorgelegd aan de klanten.

Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

Risico Management Team

Binnen de organisatie van Competentie Thermometer is een Risico Management Team verantwoordelijk voor de uitvoer van het Risico Management Programma (RMP) en het beheren van alle documenten zoals genoemd in de Leeswijzer. Het Risico Management Team bestaat uit:

- **Data Protection Officer** (DPO) – Marten Wilmink
  Verantwoordelijk voor het Risico Management Programma en voorzitter RMT;
- **Directeur Competentie Thermometer** – Daniel Hoopman
  Verantwoordelijk voor Competentie Thermometer BV;
- **Privacy Officer** (indien noodzakelijk) – Extern
  Juridisch adviseur wet en regelgeving op het gebied van privacy en IT.

Risico Management Programma

Competentie Thermometer heeft voor het beheersen van haar Informatiebeveiligingsbeleid een Risico Management Programma (RMP) ingericht dat wordt uitgevoerd door het Risico Management Team (RMT). Dit team bestaat uit de Data Protection Officer en Directeur CT en komt iedere zes maanden bijeen voor:

- Analyse van risico's voor privacy en veiligheid binnen bedrijfsprocessen en uitvoering;
- Evaluatie van eerder geïmplementeerde verbetermaatregelen en voorstel van eventuele aanpassingen;
- Opstellen concrete actiepunten en verbetermaatregelen voor nieuwe en bestaande risico's;
- Verslaglegging (verantwoordelijkheid DPO);

De aanpak van risico's binnen het RMP is gebaseerd op de Plan-Do-Check-Act-cyclus. Dit betekent dat continu wordt gekeken naar optimalisatie van processen en beleid op het gebied van veiligheid, ontwikkeling en risico's:

- **Plan** – Analyse beveiligingsrisico's, vaststellen prioriteit en ontwerpplan van aanpak voor optimalisatie.
- **Do** - Uitvoering geplande optimalisatie;
- **Check** - Evaluatie resultaat van de optimalisatie;
- **Act** - Bijstellen aan de hand van de gevonden resultaten bij Check.

Human Resources

Alle medewerkers en partners van CT worden gescreend alvorens ze in dienst treden bij CT op basis van een **Verklaring Omtrent het Gedrag** (VOG). Deze screening zal periodiek worden uitgevoerd.

Nieuwe medewerkers van CT en externe partijen die met gevoelige informatie van CT werken, tekenen een geheimhoudingsverklaring waarin ze bevestigen dat ze de **Risico Instructie** (RI), het **Calamiteitenplan** en de **Procedure Datalek** die CT voorlegt bij indiensttreding, hebben gelezen en begrepen. De Risico Instructie bevat een overzicht van de verantwoordelijkheden die medewerkers aangaan bij indiensttreding en de bewustwording van de mogelijke consequenties van nalatigheid of bepaalde beslissingen.

Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

Alle documenten binnen het Informatiebeveiligingsbeleid worden jaarlijks bijgewerkt als onderdeel van het **Risico Management Programma**. Medewerkers en externen worden vervolgens van de aanpassingen op de hoogte gesteld. Het opfrissen van de informatie uit de IBT, het Calamiteitenplan en de Procedure Datalek is een vast onderdeel tijdens de jaarlijkse beoordelingscyclus van CT met haar medewerkers en wordt als dusdanig ook vastgelegd in het gespreksverslag.

Logische toegang

De Data Protection Officer is verantwoordelijk voor het beheer van de logische toegang tot belangrijke gegevens met betrekking tot de applicatie. Hier valt te denken aan toegangscodes, sleutels en wachtwoorden voor servers, software en databases. De logische toegang voor de verschillende onderdelen van de organisatie, zoals de software, de servers, het CRM, diverse social-mediakanalen en de website zijn vastgelegd in wachtwoord software met aparte kluizen voor verschillende niveaus en onderdelen. De directeur van Competentie Thermometer is verantwoordelijk voor de fysieke toegang tot panden, het sleutelbeleid en de alarminstallatie. Jaarlijks of indien noodzakelijk geacht, wordt de logische toegang als onderdeel van het PDCA van alle medewerkers en betrokkenen geëvalueerd en waar nodig bijgesteld. Indien gewenst kan een overzicht worden gegeven van alle personen met logische toegang.

Privacy

Met betrekking tot de privacy van gebruikers en de verwerking van gegevens is een aparte **Privacyverklaring** opgesteld. Deze is te vinden op de website van CT (https://ctmeter.nl/algemeen/privacy). Klanten van CT zijn wettelijk verplicht om in hun rol als Verwerkingsverantwoordelijke, zoals gedefinieerd in de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679) (hierna: “AVG”), een verwerkersovereenkomst aan te gaan met de Verwerker van persoonsgegevens, in dit geval CT. CT biedt hiervoor een Verwerkersovereenkomst aan die ondertekend kan worden om aan deze plicht te voldoen. In deze Verwerkersovereenkomst worden de persoonsgegevens beschreven die worden verwerkt in opdracht van de Verwerkingsverantwoordelijke.

Datalek

In geval van een datalek treedt de **Procedure Datalek** in werking en zal de aangestelde Data Protection Officer (DPO) binnen één werkdag melding maken aan de Verwerkingsverantwoordelijke over de aard, omvang en impact van het betreffende incident. Tevens zal binnen twee dagen melding nadat de verantwoordelijke persoon binnen CT er kennis van heeft genomen, het incident bij de Autoriteit Persoonsgegevens gemeld worden. Lees voor meer informatie over dit onderwerp het document Procedure Datalek. Dit document is te vinden op de website van CT (https://ctmeter.nl/algemeen/privacy).

Softwareontwikkeling

Bij het ontwikkelen van de software voor CT is veiligheid en bescherming van de (persoons)gegevens één van de belangrijkste pijlers. Naast het continu testen van de software door ontwikkelaars en testers, worden ook de best practices aangehouden op het gebied van veilige software. Het bijwerken en updaten van alle gebruikte software, frameworks en modules naar de meest recente versies is hiervan een belangrijk onderdeel.

Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

Bij aanpassingen van de software of serverconfiguratie wordt een impactanalyse uitgevoerd. Concreet worden alle wijzigingen op een acceptatieomgeving die identiek is aan de productieomgeving getest. De software wordt op de acceptatieomgeving softwarematig en handmatig getest om de werking te controleren en de impact van aanpassingen of upgrades op andere onderdelen binnen de software te analyseren. Updates worden volgens het Releasebeleid van CT uitgevoerd. Onderdeel van dit beleid is de communicatie richting gebruikers voor en na geplande update.

Beveiligingsmaatregelen

Verwerker neemt de bescherming van de Persoonsgegevens zeer serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Verwerker implementeert daartoe de volgende maatregelen met betrekking tot de software en infrastructuur:

- **Beveiligingssoftware**: virusscanner en firewall;
- **TLS** (voorheen SSL): Verwerker verstuurt Persoonsgegevens (en alle andere gegevens) via een beveiligde internetverbinding;
- **DKIM** en **SPF**: zijn twee internetstandaarden die Verwerker gebruikt om te voorkomen dat gebruikers uit naam van Verwerker e-mails ontvangt die virussen bevatten, spam zijn of bedoeld zijn om persoonlijke (inlog)gegevens te bemachtigen.

Leveranciers

Hosting

Verwerker slaat zowel applicatie als back-upgegevens op op servers van Amazon. Daartoe gebruikt Verwerker het datacentrum van Amazon in Frankfurt, Duitsland. Amazon is een bedrijf dat gevestigd is in de Verenigde Staten.

Amazon garandeert dat persoonsgegevens die in Europa worden opgeslagen nooit naar de Verenigde Staten worden getransporteerd, tenzij zij daartoe wettelijk verplicht is. Mochten er toch persoonsgegevens naar de Verenigde Staten worden getransporteerd, dan garandeert Amazon dat op die gegevensverwerking in de Verenigde Staten hetzelfde strenge privacy-regime van toepassing is als in Europa. Om deze garantie te kunnen bieden is Verwerker met Amazon een overeenkomst aangegaan (**AWS Data Processing Addendum**) die Amazon heeft laten goedkeuren door de Europese privacy toezichthouders.

De Persoonsgegevens van de gebruikers worden dus ook op deze servers opgeslagen. Persoonsgegevens in de database zullen worden opgeslagen op servers in Nederland en zullen niet worden gekopieerd of verplaatst naar servers in landen waar een minder streng privacy-regime heerst dan in Europa.

Via de volgende link is na te lezen hoe Amazon de bescherming van persoonsgegevens garandeert:
https://aws.amazon.com/compliance/data-privacy-faq/

Competentie Thermometer
Bosakker 5
1901 ZL Castricum
Nederland

Certificering

De hosting servers van Amazon zijn onder andere **ISO 9001** en **ISO 27001** gecertificeerd. Bekijk voor een volledig overzicht van alle certificeringen de compliance pagina van Amazon op: https://aws.amazon.com/compliance/

Bedrijfscontinuïteit

Voor het borgen van de bedrijfscontinuïteit is met een partner (Escrow4All) een proces ingericht waarin jaarlijks broncode, access en maintenance checks worden uitgevoerd. In het geval van faillissement of ongevallen, zal de applicatie drie maanden volgens de gebruikelijke standaarden blijven werken. Hierin is het waarborgen van data ons grootste belang. Het advies aan klanten is ook om met enige regelmaat zelf exports van gegevens te maken uit de applicatie. Indien klanten een Escrow-certificaat willen ontvangen en dit proces in gang willen zetten, dan is dat tegen vergoeding mogelijk.