



## Klare Koek neemt informatiebeveiliging serieus en gaat zorgvuldig met jouw data om. Om dit te borgen hebben we een Information Security Management System ingericht.

### ISO27001 en NEN7510

Gebakken lucht doen we niet aan. Elk jaar voert een externe partij een audit bij ons uit en toetst ons op de ISO27001 en NEN7510 normen.

- **ISO27001** is een norm voor informatiebeveiliging.
- **NEN7510** is voor het verwerken van medische gegevens.

## ☰ Maatregelen

### 🎓 Opleiding, bewustwording en scholing personeel

Al onze medewerkers volgen regelmatig opleidingen op het gebied van informatiebeveiliging en worden gescreend. We maken ze weerbaar tegen bijvoorbeeld phishing en bewust hoe je met vertrouwelijke informatie omgaat. En in veel overleggen is informatiebeveiliging een vast onderdeel.

Alle medewerkers gebruiken sterke wachtwoorden, 2FA en weten hoe je veilig informatie deelt, welke software, diensten & leveranciers gebruikt mogen worden.

### ⚠️ Omgaan met risico's

Klare Koek heeft een beleid om risico's te beperken tot een acceptabel niveau. Hiervoor doen we risico analyses en kijken we naar de kans en impact van risico's. Als het nodig is nemen we maatregelen het risico te beperken. Soms accepteren we een risico, maar dan wel met goede onderbouwing en regelmatige evaluatie.

### 🚗 Een (beveiligings)incident of datalek

In het geval van een beveiligingsincident of datalek hebben we een straf recept waar niet van mag worden afgeweken. Wettelijke en contractuele verplichtingen zijn altijd in beeld en de lijntjes naar instanties als het ABP kort.

In ons bedrijfscontinuïteitplan staat uitgeschreven om in het geval van een incident werkzaamheden weer zo snel mogelijk te hervatten of op te starten.

**Datalek melden?** Stuur een mail naar [support@klarekoek.nl](mailto:support@klarekoek.nl) of bel 058 203 80 40.

### 👨‍💻 Software ontwikkeling

Software ontwikkeling en wijzigingen in bestaande software gaat volgens een vast proces om risico op

kwetsbaarheden en fouten te minimaliseren. Ook wordt er regelmatig getest op kwetsbaarheden, soms intern, soms door een externe partij.

### 📊 Monitoring en logging

We houden samen met onze leveranciers onze systemen goed in de gaten. Logs worden gecontroleerd op inconsistenties en in het geval van een incident kan worden teruggehaald hoe, wat en wanneer.

### 🗣️ Support & wijzigingen

Verzoeken om support of wijzigingen in software leggen we vast in ons ticket-systeem. We volgen daarbij een vast proces om wijzigingen zo goed & veilig mogelijk door te voeren. Er volgt standaard een evaluatie om te kijken of de klant tevreden is met de oplossing.

## 🗄️ Jouw data

### ✅ Staat in Nederland

Data die persoonsgegevens bevatten slaan we zoveel mogelijk op bij Nederlandse partijen op Nederlandse servers.

### ✅ AVG/GPDR

Bij verwerken van jouw data volgen we de AVG/GPDR.

## 🔄 Continu verbeteren

Ons informatiemanagement systeem is continu in ontwikkeling. Dat doen we volgende de Plan Do Check Act cyclus.

Zie jij dingen die we beter kunnen doen? Laat het ons weten!