Algemene informatie

In dit eerste onderdeel verzamelen we kerngegevens over uw organisatie en de contactpersoon die betrokken is bij onze samenwerking.

1 Wat is de officiële naam van uw organisatie?
2 Welke dienst(en) of welk product levert u aan VeiligheidNL?
3 Wie is binnen uw organisatie het primaire aanspreekpunt voor deze samenwerking?

Verwerking van gegevens

Hier gaan we dieper in op hoe uw organisatie omgaat met gegevens die binnen onze samenwerking worden verwerkt. We willen inzicht krijgen in de processen, verantwoordelijkheden en waarborgen die hierbij horen.

4 Verwerkt u in het kader van uw dienstverlening persoonsgegevens voor VeiligheidNL?

5 Verwerkt u bijzondere persoonsgegevens, zoals gezondheidsgegevens?
6 Maakt u gebruik van subverwerkers of onderaannemers?
6.1 Welke subverwerkers of onderaannemers zet u in, en voor welke werkzaamheden?
7 In welke landen worden gegevens opgeslagen of verwerkt?

Kwaliteitsborging (ISO 9001 gerelateerd)

Dit onderdeel onderzoeken we hoe uw organisatie de kwaliteit van haar diensten structureel waarborgt. We kijken naar beleid, processen en maatregelen die bijdragen aan betrouwbare en consistente dienstverlening.

8 Beschikt uw organisatie over een kwaliteitsmanagementsysteem?
9 Hoe borgt u dat uw dienstverlening voldoet aan gemaakte afspraken (bijv. SLA's, interne controles)?
10 Hoe registreert en behandelt u klachten of meldingen van klanten?
11 Op welke wijze evalueert en verbetert u uw dienstverlening structureel?

Informatiebeveiliging (NEN 7510 / AVG gerelateerd)

Dit onderdeel richt zich op de manier waarop uw organisatie informatiebeveiliging heeft ingericht. We vragen naar maatregelen, protocollen en verantwoordelijkheden die de veiligheid van gegevens binnen de samenwerking met VeiligheidNL ondersteunen.

12 Beschikt uw organisatie over een formeel informatiebeveiligingsbeleid?
13 Bent u gecertificeerd voor een informatiebeveiligingsnorm?
14 Hoe is toegangsbeheer ingericht (autorisaties, uitdiensttreding, periodieke controle)?

15 Beschikt u over een formeel proces voor het melden en afhandelen van beveiligingsincidenten en datalekken?
16 Binnen welke termijn meldt u een mogelijk datalek aan klanten?
17 Hoe zijn back-ups geregeld en hoe vaak worden deze getest?
18 Heeft u maatregelen getroffen voor bedrijfscontinuïteit bij uitval van systemen?

Incidenten en betrouwbaarheid

Tot slot vragen we naar eventuele incidenten, verstoringen of risico's die zich het afgelopen jaar hebben voorgedaan.

19 Hebben zich in de afgelopen 12 maanden beveiligingsincidenten voorgedaan die relevant zijn voor VeiligheidNL?

20 Zijn er in de afgelopen 12 maanden significante verstoringen geweest in uw dienstverlening? Zo ja, toelichten.

Beëindiging en gegevensoverdracht

Dit onderdeel gaat in op de afspraken en procedures rondom het beëindigen van de dienstverlening.

21 Beschikt u over een procedure voor beëindiging van de dienstverlening waarbij gegevens worden teruggeleverd en aantoonbaar verwijderd? Graag toelichten.

Verklaring

U bevestigt dat de verstrekte informatie correct en volledig is. Hieronder vult u uw naam, functie en datum in ter ondertekening van deze verklaring.

Wij kunnen aanvullende documentatie opvragen, zoals certificaten, auditrapporten (bijv. ISAE 3402 / SOC 2), informatiebeveiligingsbeleid of een continuïteitsplan.