Clarixy
24/7 Glasservice

Privacybeleid

Breng buiten naar binnen

Inhoudsopgave

Inhoudsopgave 2

1. Aanleiding/inleiding 3
2. Ambitie, doel en scope beleid 3
3. Strategische en tactische uitgangspunten 4
4. Verantwoordelijkheid Informatiebeveiliging en Privacy 5
5. Categorieën persoonsgegevens 6
6. Verwerkingsactiviteiten 8
7. Rechten van betrokkenen 8
8. Doorgiften 9

1. Aanleiding/inleiding

Elke organisatie heeft een verantwoordelijkheid met betrekking tot het omgaan met vertrouwelijke gegevens. Clarixy is daarin niet anders.

Clarixy verwerkt veel informatie en gegevens van de melder van glasschade (bewoner of opdrachtgever). Deze informatie moet goed worden beveiligd (informatiebeveiliging) en er moet op passende wijze mee om worden gegaan (privacy). Dit vraagt wat van zowel Clarixy als van individuele medewerkers.

Aan de ene kant mag privacygevoelige informatie onder geen beding openbaar worden gemaakt. Aan de andere kant is het van belang dat de medewerkers die dat nodig hebben, beschikken over betrouwbare gegevens. De situatie moet ook werkbaar blijven.

In dit document wordt beleid en een aanpak vastgesteld om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie op een passende wijze en blijvend te borgen en daarbij te voldoen aan de wettelijke regeling rondom bescherming van persoonsgegevens.

2. Ambitie, doel en scope beleid

Als Clarixy vinden wij dat cliënten, medewerkers en partners erop moeten kunnen vertrouwen dat wij zorgvuldig en veilig met hun persoonsgegevens omgaan.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen en verschillende vormen van samenwerking stellen steeds zwaardere eisen aan de bescherming van gegevens en privacy. Clarixy is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Door middel van dit beleid wordt een duidelijke richting gegeven aan informatiebeveiliging en privacy en laat Clarixy zien dat zij de privacy waarborgt, beschermt en handhaaft.

Ambitie

De ambitie bij dit beleid is om de ambities haalbaar te houden door ze te baseren op beschikbare kennis, leervermogen en kunde van de medewerkers. Het groeiproces wordt zodoende een geleidelijk leerproces, waarbij Clarixy haar medewerkers actief zal betrekken. Voor Clarixy is het belangrijk om eerst te zorgen voor overeenstemming over gezamenlijke ambities, voordat Clarixy de stap maakt naar implementatiestrategieën en -plannen. Clarixy denkt vanuit mensen en niet alleen vanuit de inhoud of verplichtingen. De haalbaarheid van de ambitie om privacy te borgen hangt nauw samen met de redenen om de privacy te beschermen. Bij Clarixy is dat een gedeelde ambitie: één zwakke schakel kan immers het hele privacybeleid teniet doen.

Het creëren van overzicht op waar en door wie welke persoonsgegevens worden verwerkt, is voor Clarixy een randvoorwaarde voor transparantie. Het hanteren van een architectuur, waarbij een overzicht wordt gegeven van de

opgeslagen en gebruikte persoonsgegevens, de gegevensstromen en de verwerkingen met hun doelbindingen is een beproefde manier om inzicht te kunnen geven.

Het nakomen van de interne afspraken ten aanzien van privacy vraagt om een eindverantwoordelijke voor privacy en het borgen van de ambities op organisatieniveau. Clarixy heeft daar een Team voor samengesteld met de Project Manager als eindverantwoordelijke.

Doelen

Doelen die daarvoor gesteld worden zijn:

- Op positieve wijze vertrouwen en vertrouwelijkheid uitstralen;
- De ambitie voor het beschermen van de privacy is duidelijk, wordt gecommuniceerd naar alle disciplines en wordt begrepen en omarmd;
- Afscherming, Corrigeerbaarheid en Transparantie is voor Clarixy belangrijk; persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.
- Zorgen voor overeenstemming over de gezamenlijke doelen en ambities, voordat Clarixy de stap maakt naar implementatiestrategieën en plannen;
- De doelen van de verwerking, de daarbij geldende wet- en regelgeving en het overzicht op de verwerkingen zijn input voor gegevensmanagement en worden gebruikt om de doelen scherp en duidelijk te houden;
- Het beperken van de bewaartermijn van persoonsgegevens moet ertoe leiden dat de gegevens niet langer worden bewaard dan nodig voor het doel of de doelen waarvoor ze zijn verzameld;
- Bij de verwerking van persoonsgegevens houdt Clarixy zich aan geldende wet aan regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)

Scope

De scope van dit beleid is als volgt:

- Het informatiebeveiligings- en privacybeleid is van toepassing op de gehele organisatie;
- Het beleid is van toepassing op de eigen medewerkers;
- Het beleid is van toepassing op de cliënten en derde partijen (zoals leveranciers en verwerkers);

Clarixy vewerkt de persoonsgegevens voor de volgende doelen:

- Een goede en efficiënte dienstverlening

3. Strategische en tactische uitgangspunten

Strategisch

Strategische uitgangspunten ten aanzien van de informatievoorziening en privacy binnen Clarixy zijn:

- De informatievoorziening moet een bijdrage leveren aan het afwikkelen van glasschades;
- Persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Deze informatievoorziening vindt ongevraagd plaats.

Dit betekent voor de informatiebeveiliging en privacy dat:

a. Deze moeten aansluiten op de strategische uitgangspunten voor informatievoorziening;
b. Eigenaarschap en verantwoordelijkheid moeten zijn belegd;
c. Het informatiebeveiligings- en het privacy beleid binnen Clarixy geldt voor alle medewerkers, cliënten, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing, leveranciers en verwerkers), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk verkregen kan worden.
d. Informatiebeveiliging en de bescherming van persoonsgegevens dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
e. Informatiebeveiliging en privacy bij Clarixy een continu proces is, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is;

Tactisch

Beveiligings- en privacyrichtlijnen en maatregelen moeten voldoen aan de volgende uitgangspunten.

a. Afscherming: houdt in dat persoonsgegevens worden afgeschermd voor het gebruik voor andere doelen dan de doelen waarvoor ze mogen worden gebruikt;
b. Corrigeerbaarheid: voor elke verwerking van persoonsgegevens is het mogelijk om de persoonsgegevens aan te passen of te vernietigen, indien de verwerking niet voldoet aan de eisen; bijvoorbeeld in geval van onjuiste informatie of als er geen noodzaak meer is om de informatie te bewaren;
c. Transparantie: over elke verwerking van persoonsgegevens is de volgende informatie beschikbaar: de verantwoordelijken, de categorieën persoonsgegevens, categorieën van betrokkenen, categorieën van ontvangers, doelbinding, de wettelijke grondslag, de bewaartermijnen, de beveiligingsmaatregelen en de organisatorische en technische inrichting van verwerking van de persoonsgegevens;

4. Verantwoordelijkheid Informatiebeveiliging en Privacy

Ten aanzien van de verantwoordelijkheden onderkent Clarixy de volgende rollen:

(Gedelegeerd) eigenaar

De Project Manager is eindverantwoordelijk voor het informatiebeveiligingsbeleid en daarmee het voldoen aan wetten en normen. De Project Manager is verantwoordelijk voor het:

- Laten uitvoeren van audits;
- Opstellen van documenten m.b.t. AVG;
- Organiseren van periodiek overleg;
- Toezien op de naleving van de Privacybeleid;
- Verzamelen van informatie ten behoeve van het toezicht binnen Clarixy om verwerkingsactiviteiten te identificeren, te analyseren en te beoordelen;
- Optreden als contactpersoon voor de Autoriteit Persoonsgegevens;
- Uitbrengen van verslagen en updates aan de CEO;

Privacy Beheerders

De Team Manager en de HR Manager zijn verantwoordelijk voor het onderhouden van het informatiebeveiligings- en het privacybeleid (dat laatste in samenwerking met de Systeem Eigenaar). De taken van de Privacy Beheerders bestaan verder uit:

- Ondersteunen van de (gedelegeerd) eigenaar;
- Het verzorgen van de jaarlijkse AVG trainingen van de medewerkers;
- Aanspreekpunt zijn voor de medewerkers;
- Het doorgeven van datalekken, of het vermoeden van datalekken aan de Gedelegeerd Eigenaar en de Systeemeigenaar;
- De medewerkers voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies;
- Het registreren en evalueren van incidenten;
- Technisch aanspreekpunt voor de Systeem eigenaar;
- Fungeren als contactpersoon voor vragen of klachten;

Systeemeigenaar

De IT Manager is verantwoordelijk voor de applicatie en bijbehorende ICT-faciliteiten. De Systeemeigenaar zorgt er voor dat zowel nu, als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving. De taken van de Systeemeigenaar bestaan verder uit:

- De gebruikersvereisten voor het systeem vaststellen en goedkeuren;
- Het bieden van nauwkeurige interpretatie van de vereiste systeemfuncties en gegevensverzamelingen;
- Het regelmatig controleren van levensduur van het systeem op naleving van AVG;
- Het vaststellen van de procedures en werkwijzen met betrekking tot het gebruik van het systeem ter ondersteuning van vakkundig gebruik van het systeem;
- Het ervoor zorgdragen dat het systeem gedurende zijn gehele levenscyclus de gegevensverwerking ondersteunt conform de wensen en eisen van de Gedelegeerd Eigenaar en de Privacy Beheerders;
- Verantwoordelijkheid dragen voor de beschikbaarheid, beveiliging, naleving, onderhoud, back-up en ondersteuning van het geautomatiseerde;
- Verantwoordelijkheid dragen voor het toezicht op de validatie van het computersysteem. Hij is uiteindelijk gedurende de hele levensduur van het systeem verantwoordelijk voor het in een gevalideerde status houden van het systeem;

5. Categorieën persoonsgegevens

Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. De gehanteerde bewaartermijnen zijn:

1. Sollicitanten

In onderstaand overzicht worden de (wettelijke) bewaartermijnen weergegeven die gelden voor gegevens c.q. documenten m.b.t. sollicitanten.

Document/gegevens	Bewaartermijn	Ingangsdatum bewaartermijn
Sollicitatiebrief, cv van sollicitant, correspondentie omtrent sollicitatie, getuigschriften, referenties, VOG	Uiterlijk 4 weken bewaard zonder toestemming óf uiterlijk 1 jaar bewaard met toestemming van de sollicitant.	Na beëindiging sollicitatieprocedure.

2. Werknemers

In onderstaand overzicht worden de (wettelijke) bewaartermijnen weergegeven die gelden voor gegevens c.q. documenten met betrekking tot werknemers.

Document/gegevens	Bewaartermijn	Ingangsdatum bewaartermijn
Arbeidsovereenkomsten (inclusief wijzigingen en aanhangsels)	Maximaal 2 jaren.	Na einde dienstverband.
Correspondentie rondom ontslag, promotie, demotie, benoemingen en sollicitatieprocedure van werknemers	Maximaal 2 jaren.	Na einde dienstverband.
Correspondentie UWV en bedrijfsarts	Maximaal 2 jaren.	Na einde dienstverband.
Gegevens zieke werknemer	Maximaal 2 jaren.	Na einde dienstverband.
Opleidingsgegevens	Maximaal 2 jaren.	Na einde dienstverband.
Verslagen functionerings- en beoordelingsgesprekken, financiële problemen werknemer, probleemsituaties	Maximaal 2 jaren.	Na einde dienstverband.
Verslagen in het kader van de Wet Verbetering Poortwachter	Maximaal 2 jaren.	Na einde dienstverband.
Kopie identiteitsbewijs	Minimaal 5 jaren.	Na het einde van het kalenderjaar waarin de dienstbetrekking is geëindigd.
Kopie identiteitsbewijs derden/ingeleende werknemers met tewerkstellingsvergunning	Minimaal 5 jaren.	Na het einde van het kalenderjaar waarin de dienstbetrekking is geëindigd.
Loonbelastingverklaringen	Minimaal 5 jaren.	Na het einde van het kalenderjaar waarin de dienstbetrekking is geëindigd.
Pensioengegevens en –stukken, burgerlijke staat, stamkaart, arbeidsvoorwaarden over samenleving en partnerschap	Minimaal 7 jaren.	Na boekjaar waarop ze betrekking hebben.
Salarisafspraken en voorwaarden	Minimaal 7 jaren.	Na einde dienstverband.

3. Klanten/cliënten en overige partijen
In onderstaand overzicht worden de (wettelijke) bewaartermijnen weergegeven die gelden voor gegevens c.q. documenten met betrekking tot cliënten/klanten en overige partijen.

Document/gegevens	Bewaartermijn	Ingangsdatum bewaartermijn
Administratieve gegevens, zoals facturen, bonnen, bankafschriften en bewijzen van uitgaven en inkomsten	Minimaal 7 jaren.	Na eerste verwerking c.q. registratie van gegevens.
Overeenkomsten van opdracht en gerelateerde documenten met persoonsgegevens van bijvoorbeeld opdrachtgevers en opdrachtnemers	Minimaal 5 jaren (in verband met aansprakelijkheid mogelijk 20 jaren)	Na eerste verwerking c.q. registratie van gegevens.
Overige gegevens van klanten/cliënten en overige partijen	Niet langer dan noodzakelijk voor het voldoen aan de verwerkingsdoeleinden.	N.v.t.

6. Verwerkingsactiviteiten

Voor elke verwerking van persoonsgegevens moet een wettelijke grondslag aanwezig zijn. Het bijhouden van een register van verwerkingsactiviteiten, inclusief gegevensmanagement, heeft tot doel ervoor te zorgen dat iedere verwerking van een persoonsgegeven aan de wettelijke vereisten voldoet én bekend is. Het register creëert overzicht, voorkomt onnodige gegevensuitwisseling, zowel intern als extern. De doelen en de activiteiten van de verwerking, de daarbij geldende wet- en regelgeving en het overzicht op de verwerkingen zijn input voor gegevensmanagement en worden gebruikt om de doelen en activiteiten scherp en duidelijk te houden. Clarixy heeft dan ook een overzicht van hoe en door wie gegevens worden verzameld en verwerkt.

Zie het Register van verwerkingen.

7. Rechten van betrokkenen

Betrokkenen hebben de volgende rechten:
- Recht op informatie: Betrokkenen hebben het recht om te vragen of, en welke persoonsgegevens van hem/haar worden verwerkt.
- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.

- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen om dit te corrigeren.
- Recht van verzet: Betrokkenen hebben het recht te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. Hieraan zal worden voldaan, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Als verwerkingsverantwoordelijke neemt Clarixy passende maatregelen opdat de betrokkene de informatie en de communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt. De informatie wordt schriftelijk of met andere middelen, met inbegrip van elektronische middelen, verstrekt. Indien de betrokkene daarom verzoekt, kan de informatie mondeling worden meegedeeld, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is.
Clarixy verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken kan die termijn met twee maanden worden verlengd.
Clarixy stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.“ Wanneer Clarixy geen gevolg geeft aan het verzoek van de betrokkene, delen wij deze laatste onverwijld en uiterlijk binnen één maand na ontvangst van het verzoek mee waarom het verzoek zonder gevolg is gebleven, en informeren wij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens en beroep bij de rechter in te stellen. Aan de hand van een verzoek kan Clarixy aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

Clarixy verstrekt de informatie kosteloos.

Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag Clarixy ofwel:

a. een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan; ofwel
b. weigeren gevolg te geven aan het verzoek.

Het is aan Clarixy om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.
Het verzoek dient bij voorkeur te worden ingediend via privacy@clarixy.nl of anders per post.

8. Doorgiften

Clarixy geeft geen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie.