PRIVACYBELEID

1.1 Algemeen

In het algemeen geldt dat zorgvuldig met persoonsgegevens moet worden omgegaan. Medewerkers van Distinto moeten zich daarom bij het gebruiken van persoonsgegevens tijdens hun dagelijkse werkzaamheden bedenken dat de privacyregels van de AVG in acht worden genomen.

1.2 Begrippen

- Persoonsgegevens: dit zijn gegevens informatie met betrekking tot een geïdentificeerde of identificeerbare persoon.
- Uitsluitend geautomatiseerde individuele besluitvorming: dit is besluitvorming over de betrokkene die uitsluitend geautomatiseerd tot stand komt, dus zonder dat een mens bij die besluitvorming is betrokken.
- Bijzondere persoonsgegevens: zijn de volgende soorten persoonsgegevens:
  a. over de gezondheid;
  b. over iemands ras of etnische achtergrond;
  c. over iemands geloof of levensovertuiging;
  d. over iemands seksuele gedrag of gerichtheid;
  e. over iemands politieke opinies;
  f. over iemands lidmaatschap van een vakbond;
  g. genetische kenmerken;
  h. biometrische kenmerken bedoeld om iemand te identificeren.
- Ook het BSN en strafrechtelijke gegevens gelden als bijzonder persoonsgegeven die alleen mogen worden gebruikt als daar een in de AVG genoemde uitzondering voor geldt.
- Verantwoordelijke: de verantwoordelijke is de partij die bepaalt wat er met de persoonsgegevens gebeurt en hoe dat gebeurt (deze bepaalt het doel en de middelen).
- Betrokkene: een betrokkene is een persoon op wie de persoonsgegevens betrekking hebben.
- Verwerking: een verwerking is een handeling met de persoonsgegevens. Daaronder valt o.a.: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden, combineren, afschermen wissen of vernietigen.
- Grondslag: voor iedere verwerking van persoonsgegevens is grondslag nodig.

1.3 Verzamelen, ontvangen en intern gebruiken van persoonsgegevens

Bij het verzamelen/creëren van persoonsgegevens, het ontvangen van persoonsgegevens van externe partijen en het verder intern verwerken daarvan binnen de organisatie wordt door Distinto een afweging gemaakt of het wettig is en hoever het gebruik kan gaan. Daarbij wordt minimaal rekening gehouden met de volgende vragen:

- Gaat het om bijzondere persoonsgegevens? Dan mogen deze alleen worden verzameld, ontvangen en verwerkt op basis van een wettelijke uitzondering. Als de bijzondere persoonsgegevens mogen worden verwerkt, geldt dat extra voorzichtig met deze persoonsgegevens moet worden omgegaan.
- Gaat het om persoonsgegevens van kinderen (personen onder de 16 jaar)? Dan moet ook extra voorzichtig met de gegevens worden omgegaan en gelden er extra regels.
- Is er een grondslag om de persoonsgegevens te verzamelen, te ontvangen en te gebruiken? Er moet voor iedere verwerking een grondslag zijn.
- Voor welke doeleinden worden de persoonsgegevens verzameld, ontvangen en verwerkt? De doeleinden moeten duidelijk en vastgelegd zijn.

- Is het noodzakelijk om de persoonsgegevens te verzamelen, te ontvangen en verder te verwerken voor de vastgestelde doeleinden? Als het niet noodzakelijk is voor die doeleinden of voor verenigbare doeleinden, dan zouden de gegevens niet moeten worden verzameld, ontvangen of verwerkt.
- Wordt er gebruik gemaakt van uitsluitend geautomatiseerde individuele besluitvorming, waaronder profiling, die rechtsgevolgen heeft voor de betrokken personen of die de personen op een andere manier in aanzienlijke mate raakt? Dit mag alleen onder bepaalde voorwaarden.
- Waar nodig voert Distinto een privacy toets uit om antwoord te geven op de bovenstaande vragen.

1.4 Register van verwerkingsgegevens

Distinto houdt intern een register van verwerkingsgegevens bij van de verschillende verwerkingen waarvoor Distinto is aan te merken als verantwoordelijke. Als Distinto is aan te merken als verwerker van bepaalde persoonsgegevens, wordt ook een overzicht bijgehouden van de verwerkingen waarvoor Distinto is aan te merken als verwerker.

1.5 Geheimhouding

Medewerkers van Distinto houden de persoonsgegevens geheim en gebruiken deze alleen in het kader van hun werkzaamheden voor Distinto. Zij verbinden zich hier schriftelijk toe richting de organisatie.

1.6 Datakwaliteit

De organisatie streeft ernaar dat persoonsgegevens up-to-date, juist en volledig zijn.

1.7 Privacy ‘by design’ en ‘by default’

Bij het ontwikkelen van (nieuwe) producten of diensten, waaronder IT-systemen wordt zoveel mogelijk gebruik gemaakt van privacy by design en privacy by default.
Privacy by design houdt samengevat in dat waar mogelijk rekening wordt gehouden met de bescherming van persoonsgegevens, bijvoorbeeld door gegevens te pseudonimiseren en dat er wordt gezorgd voor dataminimalisatie en voor naleving van de privacyregels.
Privacy by default houdt samengevat in dat er voor wordt gezorgd dat als uitgangspunt alleen noodzakelijke persoonsgegevens worden gebruikt, dit gezien de hoeveelheid persoonsgegevens, de manier waarop zij worden gebruikt, de termijn waarbinnen ze worden opgeslagen en de toegankelijkheid daarvan. De maatregelen moeten er voor zorgen dat de persoonsgegevens als uitgangspunt niet zonder dat een medewerker van Distinto daaraan te pas komt aan een onbeperkt publiek beschikbaar wordt gemaakt (bijvoorbeeld op het internet).

1.8 PIA’s (Privacy Impact Assessments) en privacytoetsen

Bij het gebruik van persoonsgegevens met een hoog risico wordt een privacy impact assessment (PIA) gedaan om na te gaan of aan de privacyregels wordt voldaan. Dit gebeurt in ieder geval bij grootschalig gebruik van bijzondere persoonsgegevens, van geautomatiseerde individuele besluitvorming (waaronder profiling) die rechtsgevolgen heeft voor de betrokken personen of die personen op een andere manier in aanzienlijke mate raakt, of van het systematisch monitoren van een publieke ruimte op grote schaal.

Bij nieuwe projecten waarbij persoonsgegevens worden verwerkt, wordt een privacytoets gedaan om na te gaan of aan de privacyregels wordt voldaan. De Functionaris gegevensbescherming (FG) wordt betrokken bij het uitvoeren van de PIA en de privacytoets.

1.9 Extern gebruik van persoonsgegevens

Als uitgangspunt geldt dat Distinto de persoonsgegevens alleen voor zichzelf gebruikt. In bepaalde gevallen kan het echter noodzakelijk zijn persoonsgegevens aan externe partijen door te geven. Bij het doorgeven van de persoonsgegevens aan externe partijen moet worden afgewogen of dat kan - en zo ja, onder welke voorwaarden:

- Is de externe partij aan te merken als een verwerker die uitsluitend handelt in opdracht van Distinto bij het in ontvangst nemen en gebruiken van persoonsgegevens? Dan worden er in een verwerkersovereenkomst afspraken gemaakt met een dergelijke partij over hoe ze met de persoonsgegevens omgaan. Dergelijke partijen mogen de persoonsgegevens niet voor eigen doeleinden gebruiken.
- Is de externe partij zelf aan te merken als verantwoordelijke, bijvoorbeeld de verzekeraar van Distinto? Dan moet worden getoetst of het doorgeven van persoonsgegevens aan deze externe partij overeenstemt met de vastgestelde doeleinden, welke persoonsgegevens daar noodzakelijk voor zijn en of er een grondslag is voor het doorgeven van de gegevens. Waar mogelijk worden afspraken vastgelegd over de uitwisseling van de persoonsgegevens.
- Is de externe partij voor de betreffende verwerking van persoonsgegevens aan te merken als verantwoordelijke samen met Distinto? Dan worden de afspraken over de persoonsgegevens vastgelegd in een overeenkomst tussen Distinto en de andere verantwoordelijke.
- Is de externe partij een overheidsinstantie? Als uitgangspunt geeft Distinto alleen persoonsgegevens aan overheidsinstanties door wanneer zij daartoe wettelijk verplicht is. In bepaalde specifieke situaties kan Distinto echter ook genoodzaakt zijn persoonsgegevens door te geven aan een overheidsinstantie als er geen wettelijke verplichting is. Een voorbeeld hiervan is het doorgeven van gegevens over een persoon aan de politie als Distinto aangifte doet tegen deze persoon. Er worden niet meer gegevens doorgegeven dan noodzakelijk.

1.10 Doorgifte naar buiten de EER

Als persoonsgegevens worden doorgeven naar een land buiten de Europese Economische Ruimte (EER), waar geen passend beschermingsniveau voor de privacy is, worden maatregelen getroffen om die doorgifte juridisch mogelijk te maken.

1.11 Beveiliging en datalekken

Persoonsgegevens moeten technisch en organisatorisch worden beveiligd op een passende manier, rekening houdend met de aard van de gegevens, de risico's van het gebruik van de persoonsgegevens, de kosten van beveiliging en de stand van de techniek. Distinto hanteert hiervoor een beveiligingsbeleid. Als zich datalekken voordoen waarbij persoonsgegevens zijn betrokken, worden deze, als dat nodig is, gemeld aan de Autoriteit Persoonsgegevens en de betrokken personen. Er kunnen bijzondere omstandigheden zijn waaronder melding niet plaatsvindt.

1.12 Bewaren persoonsgegevens

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor ze zijn verzameld. Waar toepasselijk wordt een bewaarbeleid en/of bewaarprotocol opgesteld.

1.13 Rechten van de personen

De personen om wiens persoonsgegevens het gaat kunnen met betrekking tot hun persoonsgegevens bepaalde rechten richting Distinto uitoefenen. Het gaat om de volgende rechten:

- Een overzicht in begrijpelijke vorm te ontvangen van de persoonsgegevens;
- Informatie te ontvangen over het gebruik van de persoonsgegevens door Distinto;
- Een kopie te ontvangen van de persoonsgegevens;
- In bepaalde gevallen de gegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen en op verzoek aan een andere verantwoordelijke te laten doorzenden;
- Correctie van onjuiste gegevens en aanvulling van onvolledige gegevens;
- In bepaalde gevallen om verwijdering te vragen van hun persoonsgegevens;
- In bepaalde gevallen om beperking te vragen van hun persoonsgegevens;
- In bepaalde gevallen om bezwaar te maken tegen het verwerken van hun persoonsgegevens;
- Bij gebruik van persoonsgegevens voor direct marketing doeleinden geldt dat de persoon zich altijd mag verzetten en dat gebruik wordt gestaakt;
- Als uitgangspunt om een eenmaal gegeven toestemming weer in te trekken;
- Om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

In bepaalde gevallen mag Distinto een verzoek afwijzen, bijvoorbeeld als de persoon verzoekt om verwijdering van bepaalde persoonsgegevens maar deze nog moeten worden bewaard ten behoeve van een wettelijke verplichting. Distinto stelt de persoon hiervan op de hoogte. Waar van toepassing wordt een protocol gemaakt voor het omgaan met verzoeken van de personen.

1.14 Informeren personen

De personen worden waar nodig geïnformeerd omtrent het gebruik van hun persoonsgegevens, bijvoorbeeld door middel van privacyverklaringen.

1.15 Protocollen / Richtlijnen / Gedragscodes

Bij gebruik van persoonsgegevens met een ingrijpend karakter of een andere activiteit die aanzienlijk op de privacy van de personen ingrijpt, wordt als uitgangspunt een protocol, richtlijn en/of gedragscode opgesteld waarin wordt vastgelegd hoe met de gegevens en privacy om wordt gegaan.

1.16 Training en bewustwording

Distinto probeert zo veel mogelijk bewustwording te creëren over hoe met de persoonsgegevens om moet worden gegaan. Waar toepasselijk worden trainingen gegeven om de medewerkers te informeren.

1.17 Functionaris Gegevensbescherming (FG)

Distinto heeft een Functionaris Gegevensbescherming (FG). De FG dient (minimaal) als vraagbaak voor vragen over het gebruik van persoonsgegevens (zowel voor medewerkers van Distinto als de betrokkenen), verstrekt advies over uit te voeren PIA´s en ziet toe op de naleving daarvan, ondersteunt bij projecten waarbij persoonsgegevens worden gebruikt en houdt intern toezicht op het gebruik van de persoonsgegevens door Distinto.

1.18 Wijzigingen privacybeleid

Dit privacybeleid kan worden aangepast, bijvoorbeeld om (beter) aan te sluiten op nieuwe wet- en regelgeving of gewijzigde omstandigheden. De FG wordt actief bij wijzigingen betrokken. Stakeholders worden over belangrijke wijzigingen geïnformeerd.