

Nr.	Vragen	Redenering
1	Hebben gebruikers toestemming gegeven voor het verwerken van gegevens en weten ze dat dit noodzakelijk is voor het doel waarvoor de app wordt gebruikt?	Art.6 GDPR Rechtmatigheid van de verwerking
2	Welke categorieën persoonsgegevens verwerkt u?	Afhankelijk van de categorieën verwerkte persoonsgegevens zijn er verschillende GDPR-bepalingen van toepassing
3	Gebruikt u de gegevens van de gebruiker voor verdere verwerking?	Volgens overweging 50 mag de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, alleen worden toegestaan als de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Mogelijke criminele handelingen of bedreigingen van de openbare veiligheid door de verwerkingsverantwoordelijke en het doorgeven van de relevante persoonsgegevens in individuele gevallen of in verschillende gevallen met betrekking tot dezelfde strafbare feiten of bedreigingen van de openbare veiligheid aan een bevoegde autoriteit, moet worden beschouwd als zijnde in het legitieme belang dat wordt nagestreefd door de controller. Dergelijke overdracht in het gerechtvaardigde belang van de verwerkingsverantwoordelijke of verdere verwerking van persoonsgegevens moet worden verboden als de verwerking niet verenigbaar is met een wettelijke, professionele of andere bindende geheimhoudingsplicht.
4	Verstrekt u informatie aan uw gebruikers over hoe alle gegevens door u worden verwerkt?	Artikel 13 GDPR-gegevenscontrollers moeten de betrokkenen voldoende informatie over de verwerking verstrekken
5	Verstrekt u informatie aan uw gebruikers over eventuele andere doeleinden van gegevensverwerking dan voor de oorspronkelijke doeleinden?	Artikel 13. GDPR lid 3. Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.
6	Kan de gebruiker eenvoudig zijn / haar gegevens bekijken?	Art 2: GDPR Deze verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens
7	Heeft u een DPO (Data Protection Officer) aangesteld?	Artikel 37 GDPR vereist dat verwerkingsverantwoordelijken een DPO aanstellen wanneer aan bepaalde voorwaarden is voldaan
8	Heeft u uw werknemers naar behoren gemachtigd om persoonsgegevens te verwerken?	Artikel 29 AVG elke persoon die onder het gezag van de verwerkingsverantwoordelijke handelt, moet worden geïnstrueerd om persoonsgegevens te verwerken
9	Heeft u uw relatie met externe gegevensverwerkers naar behoren geregeld via een gegevensverwerkingsovereenkomst, een Data Pro-code of een Data Pro-verklaring?	Artikel 28 GDPR-verwerking door een verwerker wordt geregeld door een contract of andere rechtshandeling (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/data_pro_code_nederland_ict.pdf) Een gegevensverwerkingsovereenkomst (DPA) is een juridisch bindend document dat schriftelijk of in elektronische vorm moet worden aangegaan tussen de verantwoordelijke en de verwerker. Het regelt de bijzonderheden van gegevensverwerking - zoals de reikwijdte en het doel ervan - evenals de relatie tussen de controller en de processor.
10	Selecteer aan welke rechten van de gebruikers u bij gegevensverwerking voldoet.	De AVG biedt de volgende rechten voor individuen: Recht op informatie, recht op toegang, recht op rectificatie, recht op verwijdering, recht op beperking van verwerking, recht op overdraagbaarheid van gegevens, recht op bezwaar en rechten met betrekking tot geautomatiseerde besluitvorming en profilering .
11	Hoe informeert u gebruikers wanneer u wijzigingen aanbrengt in het privacybeleid of hoe u persoonlijke informatie verzamelt, gebruikt of openbaar maakt.	Chapter 8: APP 8 legt specifieke verplichtingen op over het verzenden van persoonlijke informatie (https://www.oaic.gov.au/privacy/guidance-and-advice/mobile-privacy-a-better-practice-guide-for-mobile-app-developers/) https://blog.iusmentis.com/2011/06/29/voortgezet-gebruik-van-deze-site-impliceert-akkoord-met-de-voorwaarden/
12	Heeft u procedures om acties te ondernemen op verzoeken of klachten van gebruikers over schade of beïnvloeding die hun rechten schaden (bijv. Helpdesk, speciale e-mailboxen)?	Betrokkenen hebben recht op verschillende rechten (geïdentificeerd door Art. 15-22 GDPR) met betrekking tot de verwerking van hun persoonlijke gegevens. (https://www.privacy-regulation.eu/nl/artikel-7-voorwaarden-voor-toestemming-EU-AVG.htm https://www.thuiswinkel.org/bedrijven/belangenbehartiging/privacy/algemene-verordening-gegevensbescherming/toestemming)
13	Kan de gebruiker eerder gemaakte toestemmingen intrekken op dezelfde manier waarop deze zijn gegeven?	https://www.privacy-regulation.eu/en/article-7-conditions-for-consent-GDPR.htm https://www.thuiswinkel.org/companies/belangenbehartiging/privacy/al GENERAL-regelgeving- gegevensbescherming / toestemming

14	Welke verschillende persoonlijke aspecten gebruikt u voor het functioneren van uw App in de gegevensverwerking van uw gebruikers?	Overweging 71 - De betrokkene moet het recht hebben niet te worden onderworpen aan een besluit, dat een maatregel kan omvatten, waarbij de persoonlijke aspecten die op hem of haar betrekking hebben, worden geëvalueerd en die uitsluitend op geautomatiseerde verwerking zijn gebaseerd en juridische gevolgen voor hem of haar hebben of op vergelijkbare wijze een significante invloed op hem of haar heeft, zoals automatische weigering van een online kredietaanvraag of e-recruteringspraktijken zonder menselijke tussenkomst.
15	Gebruikt u gegevens van gebruikers om met geautomatiseerde besluitvormingstechnieken persoonlijke aspecten te analyseren, evalueren, voorspellen en/of te profileren?	Artikel 22, overweging 71 GDPR stelt dat verwerking 'profilering' omvat die bestaat uit elke vorm van geautomatiseerde verwerking van persoonsgegevens die de persoonlijke aspecten met betrekking tot een natuurlijke persoon evalueert, met name om aspecten te analyseren of te voorspellen met betrekking tot de prestaties van de betrokkene op het werk, de economische situatie, de gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of bewegingen, wanneer het juridische gevolgen voor hem of haar heeft of hem op soortgelijke wijze aanzienlijk beïnvloedt.
16	Welke stappen neemt u om ervoor te zorgen dat de gegevens rechtmatig, behoorlijk en transparant worden verwerkt?	Volgens de algemene beginselen van de AVG (art. 5 AVG) worden persoonsgegevens rechtmatig, eerlijk en op een transparante manier verwerkt (https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667)
17	Heeft u DPIA (Privacy Impact Assessments (PIA's) & Data Protection Impact Assessments (DPIA's)) uitgevoerd?	Onder Art. 35 GDPR- Verwerkingsverantwoordelijke moet een DPIA uitvoeren wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt waarschijnlijk leidt tot een hoog risico voor de rechten en vrijheden van betrokkenen. (https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667)
18	Worden er regelmatig passende technische en organisatorische maatregelen genomen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG is?	Art. 24 GDPR Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
19	Verwerkt u persoonsgegevens op grote schaal? Meer dan 5000 personen	De verwerkingsactiviteit kan als grootschalig worden beschouwd als: i) de verwerkingsactiviteit wereldwijd is; ii) De verwerkingsactiviteit betreft een groot aantal individuen; of iii) een groot volume aan persoonsgegevens wordt verwerkt.
20	Hoe lang bewaart u de persoonsgegevens van de gebruiker na het laatste gebruik?	Volgens het principe van opslag beperking worden persoonsgegevens niet langer bewaard dan nodig is voor de doeleinden waarvoor ze worden verwerkt
21	Wat doet u met de gegevens zodra ze niet langer nodig zijn voor het doel waarvoor ze zijn verkregen of nadat de bewaartermijn is verstreken?	Gegevensbewaring is een cruciaal onderdeel van de gegevensbescherming in de EU. Volgens het principe van opslag beperking mogen gegevens niet langer worden bewaard dan nodig is. Overweging 26 van de AVG stelt dat de beginselen van gegevensbescherming niet van toepassing moeten zijn op anonieme informatie, namelijk informatie die geen betrekking heeft op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zo anoniem zijn gemaakt dat de betrokkene niet of niet langer identificeerbaar is .
22	Worden bij het verwijderen van gegevens van een gebruiker ook de metagegevens verwijderd?	Metadata beschrijft andere gegevens. Het geeft informatie over de inhoud van een bepaald item. Een afbeelding kan bijvoorbeeld metagegevens bevatten die beschrijven hoe groot de afbeelding is, de kleurdiepte, de afbeeldingsresolutie, wanneer de afbeelding is gemaakt en andere gegevens. De metagegevens van een tekstdocument kunnen informatie bevatten over hoe lang het document is, wie de auteur is, wanneer het document is geschreven en een korte samenvatting van het document.
23	Is uw organisatie verantwoordelijk voor de verwerking, het beheer en de opslag van de gegevens?	https://www.kneppelhout.nl/actueel/verwerkingsverantwoordelijke-of-verwerker-het-verschil Art 28. GDPR De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.
24	Als u de persoonsgegevens doorgeeft aan derden, zijn de doorgiften dan binnen of buiten de EU?	Hoofdstuk V AVG identificeert de maatregelen die moeten worden genomen voor de overdracht van persoonsgegevens aan derde landen of internationale organisaties
25	Zijn er persoonlijke gegevens bekendgemaakt aan of toegankelijk voor derden buiten uw entiteit?	De EU-regels voor gegevensbescherming zijn van toepassing op de Europese Economische Ruimte (EER), die alle EU-landen en niet-EU-landen IJsland, Liechtenstein en Noorwegen omvat. Wanneer persoonsgegevens worden overgedragen buiten de EER, zijn er speciale waarborgen voorzien om ervoor te zorgen dat de bescherming met de gegevens meegaat.
26	Zijn de persoonlijke gegevens van de gebruiker zichtbaar voor andere gebruikers van de app?	Recht op privacy

27	Zijn de berichten / posts van de gebruiker zichtbaar voor andere gebruikers?	Recht op privacy
28	Waar worden de gegevens van de gebruiker opgeslagen?	https://www.cbc.ca/news/technology/the-safest-place-to-store-your-data-1.854465
29	Bij cloudopservice. Welk type service gebruikt u?	Cloudbeveiliging omvat het ecosysteem van mensen, processen, beleid en technologie die gegevens en applicaties beschermen die in de cloud werken.
30	In welk formaat slaat u de gegevens op?	Het opslaan van gegevens in platte tekst is kwetsbaar voor datalekken en wordt niet als veilig beschouwd.
31	Gebruik je scramble-technieken voor codering?	SHA-3 (Secure Hash Algorithm 3) is het nieuwste lid van de Secure Hash Algorithm-familie van standaarden, uitgebracht door NIST op 5 augustus 2015. [4] [5] Hoewel SHA-3 deel uitmaakt van dezelfde serie standaarden, verschilt het intern van de MD5-achtige structuur van SHA-1 en SHA-2.
32	Hoe vaak heeft zich in uw organisatie de afgelopen 5 jaar een datalek voorgedaan?	Inzicht in datalekken
33	Welke beveiligingsmaatregelen hebt u getroffen met betrekking tot de verwerking van gegevens?	Onder Art. 32 GDPR-gegevensverwerkers moeten zorgen voor een adequate bescherming van verwerkte persoonsgegevens door passende maatregelen te nemen
34	Is uw app gecertificeerd voor ISO / IEC-25000?	Internationale certificering van software kwaliteit
35	Welke categorieën geolocatiegegevens slaat u op?	Value Added Service is "elke service die de verwerking van verkeersgegevens of locatiegegevens vereist die verder gaan dan nodig is voor de verzending van een communicatie of de facturering met betrekking tot die communicatie". Verkeersgegevens in combinatie met locatiegegevens kunnen inbreuk maken op iemands privacy omdat het kan leiden tot gedetailleerde verblijfplaats van de betrokkene.
36	Welke stappen hebt u genomen om ervoor te zorgen dat de persoonlijke gegevens accuraat en up-to-date zijn?	Volgens 5 (d) GDPR De nauwkeurigheid van persoonlijke gegevens is een integraal onderdeel van gegevensbescherming. De AVG stelt dat "elke redelijke stap moet worden genomen" om gegevens te wissen of te corrigeren die onjuist of onvolledig zijn.
37	Hoe vaak per jaar test u de beveiliging van uw app en maakt u nodig aanpassingen?	Art. 32 GDPR: een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
38	Gebruikt uw ontwikkelteam een wachtwoordbeleid?	Deel van Art. 32 GDPR. gedragscode
39	Welke van de volgende principes is van toepassing op hoe privacy by design in uw organisatie wordt geïmplementeerd?	De letterlijke vertaling van privacy by design is: gegevensbescherming door ontwerp. Het idee is om al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen. Het houdt in dat er al bij de ontwikkeling van producten en diensten aandacht moet zijn voor privacy. In het bijzonder bij ICT-producten en -diensten gaat het erom dat al in het ontwikkelproces gebruik gemaakt wordt van privacy-verhogende maatregelen (ook wel privacy enhancing technologies of PET genoemd).
40	Zijn de door u gebruikte algoritmen op uw App op een voorspelbare en verifieerbare manier ontwikkeld?	De algoritmen zijn ontwikkeld op basis van tal van factoren zoals leeftijd, nationaliteit en geslacht, waardoor de betrokkenen een vooroordeel zouden kunnen krijgen. De algoritmen moeten de coderingsregels en de ontwikkeling ervan op een voorspelbare en verifieerbare manier uitleggen.
41	Vraagt u aan de gebruiker toestemming voor het gebruik van sensoren van de smartphone van de gebruiker?	Privacy beveiliging
42	Analyseert u (automatisch) server (beveiligings) logs?	AI predictive policing verwijst naar het vermogen om te voorspellen waar misdaden zullen plaatsvinden, de personen die ze zullen plegen, de soorten misdaad en wie de slachtoffers zullen zijn.
43	Installeert u cookies op apparaten van gebruikers?	Cookies van derden, permanente cookies en profilering zijn niet verplicht voor het functioneren van de applicatie / website. De betrokkene / gebruiker moet dus een optie hebben om deze cookies te weigeren.
44	Welk protocol gebruikt u tussen de app en de server?	Het is noodzakelijk dat app-ontwikkelingsbedrijven HTTP vervangen door de gecodeerde versie, d.w.z. HTTPS. Op basis van asymmetrische TLS / SSL-cryptografie stelt HTTPS ontwikkelaars in staat een hoge mate van beveiliging toe te voegen aan de gegevens die worden overgedragen. Maar dit is alleen mogelijk als u de HTTPS-connectiviteit op de juiste manier implementeert.
45	Gebruikt uw applicatie logboeken met aanpassingen en updates op het apparaat waar de app op draait?	De beste methode om gegevenslekage in dit scenario te voorkomen, is ervoor te zorgen dat uw mobiele Android-app deze logboeken niet gebruikt
46	Hoe beschermt u tegen data caching?	Deze techniek kan echter ook een van de boosdoeners zijn achter het lekken van gegevens in uw Android-applicatie. Het is dus weer belangrijk voor app-ontwikkelaars om te overwegen de juiste invoertypen in te stellen, auto-caching te blokkeren en te voorkomen dat inhoud naar het klembord wordt gekopieerd zonder bevestiging van de gebruiker.
47	Gebruikt u trackingtools van derden, zoals FB-pixels, Google Analytics en andere?	Dit betekent dat in-app-activiteiten waarschijnlijk worden gecontroleerd door derden en in welke mate?

48	Kunt u 99,97% uptime en service garantie bieden?	Kunnen klanten door het enorme verkeer van sommige apps meerdere servers bezitten of gebruiken, zodat de vereiste informatie altijd beschikbaar is?
49	Is uw applicatie getest en functioneel op lage bandbreedte? (2G)	Kunt u, dankzij verschillende verbindingsmogelijkheden, functioneren met de kleinste connectiviteit?
50	Is er ooit op bugs gezocht om te zien of gegevens kunnen worden gehackt? Zo ja, hoe lang geleden	Inzicht in beveiliging tegen hacken
51	Hoe vaak wordt uw app geüpdatet?	Het regelmatig bijwerken en oplossen van problemen toont de toewijding van de ontwikkelaar om de applicatie te verbeteren en de gebruikerservaring te verbeteren.
52	Hoe voorkomt u reverse engineering?	Code-verduistering is de techniek om de broncode van een toepassing moeilijk leesbaar en begrijpelijk te maken, zodat het voor een niet-geautoriseerde groep of persoon van derden bijna onmogelijk wordt om, met behulp van beschikbare hulpmiddelen, deze te reverse-engineeren
53	Zijn in uw software componenten van derden gebruikt die gebruikmaken van externe communicatie?	Software van derden loopt risico.
54	Welke tests hebt u uitgevoerd om de veiligheid van de app tijdens de ontwikkeling te garanderen?	Officiële beveiliging testprocedures
55	Moeten gebruikers zich identificeren bij het inloggen en waar wordt de authenticatie opgeslagen?	Multi-factor authenticatie vereist meer informatie dan een combinatie van gebruikersnaam en wachtwoord om autorisatie met vertrouwen te valideren.
56	Valideert u de input van de gebruikers?	Inputvalidatie, ook wel gegevensvalidatie genoemd, is het correct testen van elke input die door een gebruiker of toepassing wordt geleverd. Inputvalidatie voorkomt dat onjuist gevormde gegevens een informatiesysteem binnenkomen. Omdat het moeilijk is om een kwaadwillende gebruiker te detecteren die software probeert aan te vallen, moeten toepassingen alle invoer die in een systeem is ingevoerd, controleren en valideren. Inputvalidatie moet plaatsvinden wanneer gegevens worden ontvangen van een externe partij, vooral als de gegevens afkomstig zijn van niet-vertrouwde bronnen. Onjuiste invoervalidatie kan leiden tot injectie-aanvallen, geheugenlekkage en gecompromitteerde systemen.
57	Gebruikt u een plug-in voor reclamebureaus op uw applicatie / website om op maat gemaakte advertenties aan uw gebruikers te leveren?	Volgens overweging 47 GDPR kan de verwerking van persoonsgegevens voor direct marketingdoeleinden worden beschouwd als uitgevoerd voor een legitiem doel. Maar vooral bedrijven slagen niet voor de afwegingstoets.
58	Kunt u het percentage van gebruikers die uw app verlaten per maand meten?	Wanneer mensen een app installeren maar deze gedurende een bepaalde periode of na een tijdje niet gebruiken, verwijderen / verlaten ze
59	Zijn de schermen van uw app en werkt uw app op dezelfde manier op meerdere platforms zoals iOS, Android en Windows?	platformonafhankelijke functionaliteiten
60	Hoe beschrijf je de navigatie in je app?	Dit betekent hoe gemakkelijk het voor gebruikers is om binnen de app te navigeren, zijn de knoppen gemakkelijk te begrijpen, zijn het de conventionele pictogrammen of onconventioneel
61	Welke data gebruikt u voor de functionaliteit en de ethiek van uw app?	Gegevensbescherming voor ongeoorloofd gebruik andere gegevens van een gegevensdrager
62	In welke talen is uw app beschikbaar?	Ontwikkel je in meerdere talen of vertrouw je op vertalingen in de taal van de apparaten? (https://www.cbs.nl/nl-nl/achtergrond/2016/47/bevolking-naar-migratieachtergrond)
63	Heeft u een supportdesk / helpdesk beschikbaar voor uw gebruikers?	Als er problemen zijn met het gebruik van de apps?
64	Hoe kan een gebruiker problemen met de app naar u verzenden?	Kennisgevingsmogelijkheden
65	Hoelang wordt uw app op de markt en in gebruik?	Continuïteit
66	Hoeveel actieve gebruikers heeft uw app?	
67	Hebben eindgebruikers inspraak gehad in het ontwerp van uw app?	Mensgericht ontwerp
68	Hoe verloopt het proces als een gebruiker een incident meldt?	procesbetrouwbaarheid
69	Worden de GPS-locatiegegevens gedeeld met de lokale overheid / politie?	Dit is een voordeel om sneller ter plaatse te kunnen zijn en eventueel andere sensoren aan te spreken
70	Kunnen andere gebruikers de melding van een gebruiker zien?	Als ik bijvoorbeeld zojuist een nieuwe app op mijn apparaat heb geïnstalleerd, krijgen andere gebruikers een melding, en als een van mijn contacten lid wordt krijg ik een melding.

71	Ontvangt de gebruiker een bericht dat zijn rapport correct is aangekomen?	Maakt app betrouwbaar
72	Ontvangt de gebruiker een bericht dat zijn rapport is verwerkt?	Maakt app betrouwbaar
73	Kunnen gebruikers een emotionele dimensie invoeren in een rapport of bericht?	Dylan Roskams-Edris warns about the habit forming and addictive capacities of smartphone apps and explains the need for an ethics of apps. recommendations of Tristan Harris.
74	Behandelt uw app kwetsbare populatie of gevoelige onderwerpen?	Kwetsbare personen zijn bijvoorbeeld kinderen, ouderen, gehandicapten, werknemers, analfabeten en asielzoekers.
75	Bewaakt en registreert uw app het gedrag van de gebruiker?	Om te bepalen of een verwerkingsactiviteit kan worden overwogen om het gedrag van betrokkenen te volgen, moet worden nagegaan of natuurlijke personen op het internet worden gevolgd, inclusief mogelijk volgend gebruik van persoonsgegevensverwerkingstechnieken die bestaan uit het profileren van een natuurlijke persoon, met name in om beslissingen over hem of haar te nemen of om haar of zijn persoonlijke voorkeuren, gedragingen en attitudes te analyseren of te voorspellen.
76	Kunnen gebruikers in de app hun mening geven over bepaalde onderwerpen en over andere gebruikers?	Dylan Roskams-Edris warns about the habit forming and addictive capacities of smartphone apps and explains the need for an ethics of apps. recommendations of Tristan Harris.
77	Worden persoonsgegevens gebruikt voor het profileren van individuen of om ze op een schaal te scoren?	Profileren analyseert aspecten van iemands persoonlijkheid, gedrag, interesses en gewoonten om er voorspellingen of beslissingen over te nemen. U voert profilering uit als u: op grote schaal persoonsgegevens verzamelt en analyseert met behulp van algoritmen, AI of machine learning; associaties identificeren om verbanden te leggen tussen verschillende gedragingen en kenmerken; profielen maken die u op individuen toepast; of voorspel het gedrag van individuen op basis van hun toegewezen profielen.
78	Zal de verwerkingsactiviteit een systematische en uitgebreide evaluatie van persoonlijke aspecten omvatten op basis van geautomatiseerde besluitvorming?	Geautomatiseerde besluitvorming betekent dat er geen mens bij de beslissing wordt betrokken. Deze beslissingen kunnen gebaseerd zijn op feitelijke gegevens, maar ook op digitaal aangemaakte profielen of afgeleide gegevens. Een online besluit om een lening toe te kennen is een voorbeeld van geautomatiseerde besluitvorming. Bij geautomatiseerde besluitvorming gaat het vaak om profilering, maar dat hoeft niet.
79	Is uw app (automatisch) gekoppeld aan een nieuwssite of social media	Recht op privacy
80	Doet u financieel zaken met de data?	Het lijkt niet ethisch, maar een verdienmodel voor de app-ontwikkelaar is natuurlijk mogelijk
81	Welke stappen neemt u om ervoor te zorgen dat de gegevens op een transparante manier worden verwerkt? Geef aan wat van toepassing is.	Elke verwerking van persoonsgegevens moet rechtmatig, eerlijk en transparant zijn. Het moet voor individuen duidelijk en transparant zijn dat persoonsgegevens die op hen betrekking hebben, worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt, en in hoeverre de persoonsgegevens worden of zullen worden verwerkt. Het recht om geïnformeerd te worden, volgens de artikelen 13 en 14 AVG, is een essentieel onderdeel van de verplichtingen van organisaties om transparant te zijn.
82	Hoe vaak voert u een tevredenheidsonderzoek uit onder uw gebruikers?	Forbes - onderzoeksinzet van het bedrijf
83	Over welke privacy zaken heeft u contact met de gebruiker bij het gebruik van uw app?	Interactiviteit tussen leverancier en klant kan een basis leggen in vertrouwen.
84	Wat doet u na een inbreuk op de privacy?	Art. 33 GDPR Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit
85	Heeft u uw app ontwikkeld met de "Hooked" -methode?	zie https://www.youtube.com/watch?v=iw1x0zos8Jo
86	Hoe vaak bekijkt u of de gegevens nog relevant zijn naarmate uw product vordert?	Wees behendig en iteratief
87	Hoe kunt u uw organisatie beschrijven in relatie tot uw app?	Rechtvaardiging
88	Wat voor soort organisatie bent u:	Beeldvorming
89	Hoeveel medewerkers heeft uw organisatie?	Groot lijkt meer continuïteit te geven
90	Gebruikt u integriteitstoets voor screening vóór indiensttreding?	Art. 32 GDPR organisatorische maatregelen
91	Is uw werkomgeving vrij van onwettige discriminatie, intimidatie of geweld?	In artikel 1 van de Grondwet staat dat iedereen in Nederland in gelijke gevallen gelijk wordt behandeld. Verder staat in artikel 1 dat discriminatie, op welke grond dan ook, is verboden. Ook aanzetten tot haat of discriminatie is verboden.
92	Heeft uw organisatie meerdere apps ontwikkeld en op de markt gebracht?	Beeldvorming

93	Hoe is het verdienmodel van de app?	Geeft een indicatie van de zuiverheid van het businessmodel
94	Hoeveel draagt deze app bij aan uw omzet?	Afbeelding van afhankelijkheid
95	Is de broncode van uw app bij een neutrale autoriteit geplaatst om ervoor te zorgen dat als er iets met uw bedrijf gebeurt, de app verder kan worden gebruikt?	Continuïteit
96	Heeft uw organisatie ISO certificatie?	Certificering van kwaliteitsmanagement / environment, security
97	Welke maatregelen neemt u om corruptie te voorkomen?	https://knowledgehub.transparency.org/assets/uploads/helpdesk/The-relationship-between-business-integrity-and-commercial-success_2018.pdf en https://www.compliance-instituut.nl/wp-content/uploads/Corporate-Governance-Business-Integrity-2015.pdf
98	Volgt uw organisatie de richtlijnen en onderneemt zij de juiste acties voor het mensenrechten programma van de Verenigde Naties? (geen slavernij, geen kinderarbeid)	https://www.un.org/en/sections/issues-depth/human-rights/
99	Heeft u beleid om de CO2-uitstoot te verminderen en / of te compenseren?	De inzet om milieuvriendelijk te zijn, kan van invloed zijn op de betrouwbaarheid van de ontwikkelaar
100	Hoe geeft uw organisatie vorm aan goed werkgeverschap / burgerschap?	Een goede werkgever is een pluspunt bij het goed functioneren van een team