Evaluatieformulier	***ja***	***nee***	***commentaar of verwijzing naar bijgevoegde documenten***
Gebruik van persoonsgegevens uit het netwerk van de sociale zekerheid door kredietinstellingen en aanbieders van financiële producten en diensten ten behoeve van (bestaande en prospectieve) klanten – naleving van beraadslaging nr. 19/004 van 15 januari 2019 en beraadslaging nr. 19/032 van 5 februari 2019 van het informatieveiligheidscomité			
1. Gebeurt elke handeling die u verricht bij de verwerking van de persoonsgegevens in het kader van de aangeboden toepassing op initiatief en met toestemming van de betrokkene?			
2. Heeft u uitdrukkelijk met elke betrokkene afspraken gemaakt over uw onderlinge relatie (onder meer welke persoonsgegevens er over hem worden bijgehouden en de finaliteit en duurtijd van de verwerking van zijn persoonsgegevens), over de draagwijdte van uw tussenkomst en over de acties die u in het kader van de aangeboden toepassing kunt verrichten?			
3. Controleert u bij het raadplegen en het bijwerken van de persoonsgegevens in het kader van de aangeboden toepassing steeds of de toestemming van de betrokkene nog geldt?			
4. Bewaart u de bewijzen van de toestemming van de betrokkene, voor eventuele inzage door de authentieke bronnen van de in het kader van de aangeboden toepassing verwerkte persoonsgegevens, door de KSZ en/of door het IVC?			
5. Voldoet de aangeboden toepassing aan dezelfde veiligheidsstandaarden als deze die gelden voor gelijkaardige toepassingen van de overheid?			
6. Voldoet het veiligheidsniveau van de aangeboden toepassing inzake beveiligde login aan de hoogste eisen op het vlak van authenticatie (niveau 400 of hoger binnen de FAS)[1]?			
7. Gebeurt de verwerking van de persoonsgegevens in het kader van de aangeboden toepassing beveiligd en gestructureerd, tussen servers met de nodige certificaten, zoals in de sociale zekerheid?			
8. Heeft u organisatorische maatregelen getroffen waardoor de persoonsgegevens in het kader van de aangeboden toepassing enkel kunnen worden verwerkt door de daartoe aangeduide personen die er zich toe verbonden hebben om de veiligheid en de vertrouwelijkheid ervan te waarborgen en houdt u een permanent geactualiseerde lijst van die personen ter beschikking?			
9. Krijgt de betrokkene eerst op het door hemzelf geregistreerde mailadres een waarschuwing over het feit dat de aangeboden toepassing een toegang tot zijn persoonsgegevens gebruikt?			
10. Heeft u voorzien in een eenvoudig middel waarmee de betrokkene via de technologie van de Open Authorization te kennen kan geven dat er tussen hem en u een relatie bestaat?			
11. Kan de betrokkene op elk moment raadplegen welke actieve relaties er bestaan en deze eventueel beëindigen, bijvoorbeeld als reactie op de waarschuwing die hij per mail ontvangt?			

[1] Zie daartoe in het bijzonder "FAS SAML Integration Guide", hoofdstuk 6: "AUTHENTICATION MEANS" (http://dtservices.bosa.be/sites/default/files/content/download/files/fas_saml_integration_guide_v0.51_2.pdf).

12. Houdt u zich ter beschikking voor een eventuele audit door de functionaris(sen) voor gegevensbescherming van de authentieke bron(nen) van de persoonsgegevens?			
13. Verwerkt u de persoonsgegevens enkel voor het verstrekken van financieel advies en het formuleren van passende commerciële voorstellen aan de individuele betrokkenen?			
14. Vernietigt u de persoonsgegevens indien ze niet langer dienstig zijn voor die doeleinden, indien de geldigheid van de toestemming van de betrokkene is verstreken of indien de betrokkene daar uitdrukkelijk om vraagt?			
15. Vernietigt u de persoonsgegevens van prospectieve klanten met wie u uiteindelijk geen contractuele relatie aangaat uiterlijk één maand na uw precontractueel aanbod?			
16. Heeft u de nodige processen en contactmogelijkheden voorzien zodat de betrokkene u vlot kan bereiken voor vragen gerelateerd aan deze verwerking?			
Algemeen			
1. Beschikt u over een functionaris voor gegevensbescherming? Zo ja, gelieve de hierboven vermelde rubriek in te vullen?			
2. Hebt u de risico's en beveiligingsbehoeften die eigen zijn aan uw organisatie en die de verwerking van persoonsgegevens betreffen geëvalueerd?			
3. Beschikt u over een geschreven versie van uw beveiligingsbeleid en is uw beleid t.a.v. de bescherming van persoonsgegevens daarin geïntegreerd? Zo ja, dient een kopie als bijlage bij de aanvraag te worden gevoegd.			
4. Hebt u de diverse dragers van uw organisatie geïdentificeerd waarbij persoonsgegevens betrokken zijn?			
5. Zijn de interne en externe personeelsleden die bij de verwerking van persoonsgegevens betrokken zijn, goed op de hoogte van de vertrouwelijkheids- en beveiligingsplichten ten aanzien van deze gegevens die zowel voortvloeien uit de verschillende wettelijke vereisten als uit het beveiligingsplan?			
6. Hebt u beheersmaatregelen genomen ter verhindering van de niet-gemachtigde of onnodige fysieke toegang tot dragers die persoonsgegevens bevatten?			
7. Hebt u maatregelen genomen ter verhindering van elke fysieke schade die de persoonsgegevens in gevaar zouden kunnen brengen?			
8. Hebt u beheersmaatregelen genomen ter bescherming van de verschillende netwerken waarmee de apparatuur die de persoonsgegevens verwerkt, is verbonden?			
9. Beschikt u over een actuele lijst van de verschillende bevoegde personen die toegang hebben tot de persoonsgegevens en van hun respectievelijk toegangsniveau (creatie, raadpleging, wijziging, vernietiging)?			

10. Hebt u op uw informatiesystemen een mechanisme voor toegangsmachtiging geïnstalleerd zodat de persoonsgegevens en de verwerkingen die er betrekking op hebben enkel toegankelijk zijn voor de personen en toepassingen die hiertoe uitdrukkelijk gemachtigd zijn?			
11. Is uw informatiesysteem zodanig ontworpen dat de identiteit van de personen die toegang hebben gehad tot de persoonsgegevens en het type van persoonsgegevens die werden geraadpleegd permanent geregistreerd worden?			
12. Hebt u erin voorzien dat de geldigheid en de doeltreffendheid in de tijd van de ingestelde organisatorische en technische maatregelen gecontroleerd worden ter garantie van de beveiliging van de persoonsgegevens?			
13. Hebt u voorzien in urgentieprocedures en rapporteringsprocedures bij beveiligingsincidenten waarbij persoonsgegevens betrokken zijn?			
14. Beschikt u over een bijgewerkte documentatie betreffende de verschillende genomen beheersmaatregelen ter bescherming van persoonsgegevens en de verschillende verwerkingen die er betrekking op hebben?			