Formulaire d'évaluation	***oui***	***non***	***Commentaire ou référence aux documents en annexe***
Utilisation de données à caractère personnel du réseau de la sécurité sociale par les établissements de crédits et les prestataires de produits et services financiers au profit des clients (actuels et prospectifs) - respect des délibérations du Comité de sécurité de l'information n° 19/004 du 15 janvier 2019 et n° 19/032 du 5 février 2019			
1. Lors du traitement des données à caractère personnel, toute action exécutée dans le cadre de l'application proposée est-elle effectuée à l'initiative de l'intéressé et avec son consentement ?			
2. Avez-vous explicitement conclus des accords avec chacun des intéressés en ce qui concerne votre relation mutuelle (notamment quelles données à caractère personnel le concernant seront conservées, ainsi que la finalité et la durée du traitement de ses données à caractère personnel), la portée de votre intervention et les actions que vous pouvez réaliser dans le cadre de l'application proposée ?			
3. Lors de la consultation et de la mise à jour des données à caractère personnel dans le cadre de l'application proposée, vérifiez-vous toujours si le consentement de l'intéressé est toujours valable ?			
4. Conservez-vous les preuves du consentement de l'intéressé, afin que les sources authentiques des données à caractère personnel traitées dans le cadre de l'application proposée, la BCSS et/ou le CSI puissent éventuellement en prendre connaissance ?			
5. L'application proposée répond-elle aux standards de sécurité valables pour des applications similaires des autorités ?			
6. Le niveau de sécurité de l'application proposée en ce qui concerne l'ouverture d'une session sécurisée satisfait-il aux exigences les plus strictes en matière d'authentification (niveau 400 ou supérieur dans FAS)[1] ?			
7. Le traitement des données à caractère personnel dans le cadre de l'application proposée est-il effectué de manière sécurisée et structurée, entre des serveurs équipés des certificats nécessaires, à l'instar des pratiques dans la sécurité sociale ?			
8. Avez-vous prévu des mesures organisationnelles de sorte à ce que les données à caractère personnel dans le cadre de l'application proposée puissent uniquement être traitées par les personnes désignées à cet effet, qui se sont engagées à en garantir la sécurité et la confidentialité et disposez-vous d'une liste actualisée de ces personnes ?			
9. L'intéressé reçoit-il une notification à l'adresse e-mail qu'il a communiquée concernant le fait que l'application proposée a recours à l'accès à ses données à caractère personnel ?			
10. Avez-vous prévu un moyen simple permettant à l'intéressé, via la technologie de l'Open Autorization, d'indiquer qu'il existe une relation entre lui et vous ?			

[1] Voir à cet égard "FAS SAML Integration Guide", chapitre 6: "AUTHENTICATION MEANS" (http://dtservices.bosa.be/sites/default/files/content/download/files/fas_saml_integration_guide_v0.51_2.pdf).

11. L'intéressé peut-il, à tout moment, consulter les relations actives qui existent et peut-il, le cas échéant, y mettre fin, par exemple en réaction à l'avertissement qu'il a reçu par mail ?			
12. Etes-vous disponible pour un éventuel audit réalisé par le(s) délégué(s) à la protection des données des sources authentiques des données à caractère personnel ?			
13. Traitez-vous les données à caractère personnel uniquement pour fournir des avis financiers et formuler des propositions commerciales adéquates aux intéressés individuels ?			
14. Détruisez-vous les données à caractère personnel lorsqu'elles ne sont plus nécessaires pour les finalités, au terme de la validité du consentement de l'intéressé ou à la demande explicite de l'intéressé ?			
15. Détruisez-vous les données à caractère personnel des clients prospectifs avec qui vous ne concluez finalement pas de relation contractuelle et ce au plus tard un mois après votre offre précontractuelle ?			
16. Avez-vous prévu les processus et possibilités de contact nécessaires de sorte que l'intéressé puisse vous joindre facilement pour toute question relative au traitement ?			
Généralités			
1. Disposez-vous d'un délégué à la protection des données? Dans l'affirmative, veuillez remplir la rubrique précitée.			
2. Avez-vous évalué les risques et les besoins de protection qui sont inhérents à votre organisation et qui concernent le traitement de données à caractère personnel?			
3. Disposez-vous d'une version écrite de votre politique de sécurité et inclut-elle votre politique de protection des données à caractère personnel ? Dans l'affirmative, veuillez joindre une copie de cette politique en annexe de la demande.			
4. Avez-vous identifié les divers supports de votre organisation contenant des données à caractère personnel?			
5. Le personnel interne et externe concerné par le traitement de données à caractère personnel est-il suffisamment informé des obligations de confidentialité et de protection en lien avec ces données, qui découlent à la fois des différentes dispositions légales et du plan de sécurité?			
6. Avez-vous pris des mesures de gestion pour empêcher tout accès physique inutile ou non autorisé aux supports contenant les données à caractère personnel?			
7. Avez-vous pris des mesures pour éviter tout dommage physique qui pourrait compromettre les données à caractère personnel ?			
8. Avez-vous pris des mesures de gestion pour protéger les différents réseaux auxquels sont connectés les appareils qui traitent les données à caractère personnel?			

9. Disposez-vous d'une liste actuelle des différentes personnes compétentes qui ont accès aux données à caractère personnel et de leur niveau d'accès respectif (création, consultation, modification, destruction)?			
10. Avez-vous installé un mécanisme d'autorisation d'accès sur vos systèmes d'information de sorte que les données à caractère personnel traitées et les traitements qui y ont trait, soient uniquement accessibles aux personnes et applications qui y sont expressément autorisées?			
11. Votre système d'information est-il conçu de telle sorte qu'il enregistre en permanence l'identité des personnes qui accèdent aux données à caractère personnel ainsi que le type de données à caractère personnel consultées ?			
12. Avez-vous prévu de contrôler la validité et l'efficacité des mesures organisationnelles et techniques à travers le temps afin de garantir la protection des données à caractère personnel ?			
13. Avez-vous prévu des procédures d'urgence et de rapportage en cas d'incidents de sécurité impliquant des données à caractère personnel ?			
14. Disposez-vous d'une documentation mise à jour concernant les différentes mesures de gestion mises en place en vue de la protection des données à caractère personnel et des différents traitements qui y ont trait ?			