

Politique de conservation des données à caractère personnel de TF BANK

Table des matières

1. Introduction.....	2
1.1. Objet.....	2
1.2. Portée.....	2
1.3. Public cible.....	2
1.4. Définitions.....	2
2. Texte de référence.....	2
3. Lignes directrices sur la mise en œuvre.....	3
3.1. Durée maximale de conservation des données à caractère personnel.....	3
3.1.1. Période de conservation en fonction de la finalité.....	3
3.1.2. Durée de conservation selon le RGPD.....	4
3.1.3 Conservation des données à des fins probatoires.....	6
3.1.4 Exceptions.....	7
3.2. Archivage des données à caractère personnel.....	7
3.2.1. Un archivage sélectif.....	7
3.2.2. Le choix d'un mode d'archivage.....	7
3.2.3. Un archivage sécurisé.....	8
3.3. Suppression des données à caractère personnel.....	8
3.3.1. Purge automatisée ou semi-automatisée.....	8
3.3.2. Purge manuelle.....	8
3.3.3. Alternatives techniques à l'effacement des données.....	9
3.4. Obligations d'information.....	9
4. Contact.....	10
Annexe.....	11

1. Introduction

1.1. Objet

Le Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 25 mai 2018. Son article 5(e) introduit l'obligation de conserver des données à caractère personnel enregistrées seulement le temps nécessaire pour la finalité pour laquelle nous avons recueilli les données.

Ce principe est étroitement lié aux obligations d'éviter de conserver des données à caractère personnel qui sont inexacts, obsolètes ou non pertinentes. En effet, la conservation des données à caractère personnel plus longtemps que le temps strictement nécessaire à leur exploitation, cela peut causer les problèmes suivants :

- Accroître le risque de voir les données devenir obsolètes, et que ces informations obsolètes soient utilisées par erreur, au détriment de toutes les personnes concernées.
- Mettre en péril le contrôle qualité de la donnée, du fait d'une temporalité trop importante.
- Lorsque TF BANK n'a plus besoin des données à caractère personnel, nous devons nous assurer qu'elles sont conservées en toute sécurité afin d'éviter tout risque de fuite frauduleuse, d'utilisation abusive ou d'accès non autorisé.

1.2. Portée

Le RGPD définit les périodes de conservation maximale pour l'enregistrement ou le traitement, aussi bien structuré que non structuré, des données à caractère personnel.

1.3. Public cible

Tous les personnels de TF BANK.

1.4. Définitions

Tous les mots-clefs associés peuvent être trouvés dans l'article 4 du RGPD.

2. Texte de référence

RGPD Art. 5 : Principes relatifs au traitement des données à caractère personnel

(1) Les données à caractère personnel de l'utilisateur doivent être :

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles les données à caractère personnel sont traitées ; les données à caractère personnel peuvent être conservées pendant des périodes plus longues dans la mesure où elles sont traitées uniquement à des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique, ou à des fins statistiques conformément à l'article 89, paragraphe 1, sous réserve de la mise en œuvre des mesures techniques et organisationnelles appropriées requises par le présent règlement afin de sauvegarder les droits et libertés de la personne concernée (principe de « limitation de la conservation »).

3. Lignes directrices sur la mise en œuvre

3.1. Durée maximale de conservation des données à caractère personnel

Le RGPD ne définit pas de période minimum ou maximum de conservation des données à caractère personnel. Il établit que les données à caractère personnel recueillies pour n'importe quelle finalité ne doivent pas être conservées plus longtemps que nécessaire.

En outre, TF BANK respectera *également* les dispositions légales contraignantes spécifiques concernant la conservation des données applicables dans chaque pays où TF BANK opère.

Un ensemble minimal de données sera conservé à des fins de preuve.

3.1.1. Période de conservation en fonction de la finalité

Les données à caractère personnel des clients, des fournisseurs et des salariés de TF BANK seront conservées dans les registres tant que durera la relation entre TF BANK et ces personnes. Lorsque cette relation prend fin, se pose la question de la durée de conservation de leurs données à caractère personnel.

TF BANK définit des périodes de conservation standard pour toutes sortes de données à caractère personnel, car la durée de conservation dépend principalement de la finalité pour laquelle ces données ont été recueillies.

Toutefois, les périodes de conservation standard doivent être définies par catégories d'information, car certaines données à caractère personnel peuvent être effacées plus tôt que d'autres : il n'est pas nécessaire de supprimer *toutes* les données à caractère personnel à la fin d'une relation avec un client ou salarié. Certaines informations peuvent devoir être conservées (par exemple en vertu d'exigences légales).

Lors du traitement des données à caractère personnel, TF BANK doit :

- Prendre en compte la finalité pour laquelle elle a recueilli ces données, afin de décider si elles seront conservées ou non ;
- Identifier quelles informations de base doivent être conservées pendant la plus longue durée maximale, et lesquelles peuvent être effacées à un stade antérieur car leur intérêt décroît plus rapidement ;
- Ré-examiner la durée de conservation des données à caractère personnel pour chaque catégorie ;
- Etablir une procédure pour supprimer en toute sécurité des informations qui ne sont plus nécessaires à cette fin ;
- Noter dans le registre de traitement les durées de conservation choisies pour chaque catégorie de données à caractère personnel traitées.

Exemple

En tant qu'employeur, TF BANK passe en revue les données à caractère personnel qu'il détient au sujet des salariés lorsqu'ils quittent la banque. Par exemple, il doit conserver suffisamment de données pour permettre au service des Ressources Humaines de gérer les prestations de retraite.

Toutefois, les données à caractère personnel dont l'utilité future est peu probable doivent être effacées de la base de données, par exemple les coordonnées de la personne de contact d'urgence, les adresses précédentes ou les détails des bénéficiaires de leur assurance-vie, etc.

3.1.2. Durée de conservation selon le RGPD

Les dispositions légales concernant la conservation des données sont présentes dans plusieurs sources de la législation nationale : la plupart des pays fournissent une règle générale dans leur Code de commerce et le Code civil, et des règles supplémentaires dans la réglementation fiscale ou, plus rarement, dans des ordonnances spéciales pour la conservation des documents (exemple : lutte contre le blanchiment d'argent).

TF BANK choisit d'appliquer les périodes de conservation des données prévues par la loi française.

Le tableau ci-dessous montre les périodes de conservation applicables en France¹².

Effectif	Type de données	Durée de conservation des données (France uniquement)
Gestion du personnel	Registre unique du personnel	5 ans à partir du départ du salarié
	Document concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régimes de retraite	5 ans
	Document relatif aux charges sociales et à la taxe sur les salaires	3 ans
	Comptabilisation des jours de travail des salariés sous convention de forfait	3 ans
	Comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation	1 an
	Observation ou mise en demeure de l'inspection du travail. Vérification et contrôle du Comité d'Hygiène, de Sécurité et des Conditions de Travail (CHSCT)	5 ans
	Déclaration d'accident du travail auprès de la caisse primaire d'assurance maladie	5 ans
Salariés	Gestion du personnel	5 ans à compter de la date du licenciement
	Gestion des états de paie	5 ans à compter de la date de paiement du salaire

¹ Voir le référentiel relatif à la durée de conservation élaboré par la CNIL (version 2012).

² Documents listés par le Service Public : <https://www.service-public.fr/professionnels-entreprises/vosdroits/F10029>

	Dossier de recrutement (CV, diplômes, entretiens...)	Destruction immédiate si le candidat échoue Possibilité de garder le CV 2 ans après le dernier contact avec le candidat
	Vidéosurveillance	1 mois
	Répertoire (Répertoire téléphonique)	Suppression juste après le départ de la personne
	Journal du contrôle des applications	6 mois d'historique de connexion
	Contrôle de l'utilisation d'Internet et des e-mails	6 mois
	Contrôle de l'utilisation de la messagerie	6 mois
	Journal d'appels	1 an
	Géolocalisation des véhicules professionnels	2 mois
	Contrôle des horaires	5 ans après le départ de la personne pour les éléments d'identification ; 5 ans pour les informations relatives aux horaires des salariés ; 5 ans pour la conservation des données relatives aux motifs d'absence
	Contrôle d'accès aux bâtiments	Suppression immédiate si le salarié quitte l'entreprise ; 3 mois d'historique pour un salarié actif
	Sanctions disciplinaires	3 ans
	Enregistrement des conversations téléphoniques sur le lieu de travail à des fins de preuve dans le secteur bancaire	6 mois minimum/5 ans maximum
	Enregistrements des conversations téléphoniques à des fins d'entraînement	6 mois
Marketing & Commerciaux	Informations sur les prospects	Prospects, pas clients : 3 ans Prospects clients : jusqu'à la fin de la relation commerciale
	Contrats avec un marchand ou non marchand	5 ans
	Commandes	10 ans
	Livraisons	10 ans
	Factures	10 ans
	Comptabilité / gestion des comptes clients	10 ans
	Campagnes e-mailing ou appels téléphoniques...	3 ans à compter du dernier contact
	Lettre d'information	Jusqu'à désabonnement de la personne concernée
	Conservation des numéros de carte bancaire	Suppression dès le paiement effectif 13 mois pour un archivage intermédiaire pour une finalité de preuve
	Cryptogramme visuel de carte bancaire	Pas de conservation
	Liste d'opposition	3 ans à compter de l'inscription dans la liste
	Identité des clients habituels et occasionnels	5 ans à compter de la clôture du compte ou de la cessation de la relation commerciale
	Documents et informations relatives aux opérations bancaires faites par les clients (dépôt, retrait, virement, prélèvement, carte...) et leurs caractéristiques	5 ans à compter de l'exécution de l'opération
	Comptes sans opérations ni réclamations	10 ans
	Gestions des crédits ou des prêts	5 ans à compter du remboursement du crédit

Bancaire		6 mois en l'absence de conclusion du contrat
	Suivi de l'activité relative aux instruments financiers	10 ans après la fin de l'opération
	Chèques	Première délivrance de formules de chèques : trace de consultation du fichier central des chèques pendant 2 ans ; Date de remise ou d'envoi des formules de chèque au titulaire du compte : justification pendant 2 ans ; Chèques impayés : - Incidents de paiement régularisés : conservation pendant 48h à compter de la régularisation - Incidents de paiement non régularisés : conservation pendant 3 ans maximum à compter de la survenance de l'impayé ; Chèques perdus ou volés : dès la justification par le porteur : effacement des données concernant mais possibilité de conserver les numéros de chèques perdus ou volés.
	Liste d'initiés	Mise à jour des listes en cas d'accès d'une nouvelle personne à des informations privilégiées, de cessation d'accès à ces informations ou de changement de statut de la personne : le plus rapidement possible. Information enregistrées devenues caduques : 5 ans suivant la cessation ou le changement de motif.
	Abus de marché	45 jours en archivage courant puis basculent en archivage intermédiaire pendant 3 ans
	Modèle de score	6 mois en cas de refus de la demande de crédit (ou pour les prospects)
	Informations comptables	10 ans
	Fichier des incidents de remboursement des crédits aux particuliers	Dès la régularisation de la dette ou à défaut pendant 5 ans 10 ans en cas de procédure de surendettement
	Fichier des incidents de paiement par chèques et cartes bancaires	Chèques : 5 ans si non régularisé Carte bancaire : 2 ans à compter du retrait de la carte bancaire
	Lutte contre le blanchiment et le financement du terrorisme	Informations permettant de justifier de l'opération : 5 ans à compter de l'exécution de l'opération

3.1.3 Conservation des données à des fins probatoires

Il est parfois nécessaire de garder les données à caractère personnel pour que TF BANK puisse se défendre lors d'éventuels recours juridiques entrepris soit par les clients, les (ex-)salariés, les fournisseurs, l'administration...

Toutefois, TF BANK peut toujours supprimer les informations qui pourraient ne pas être pertinentes pour un tel recours (principe de minimisation des données). À moins qu'il y ait une autre raison de les conserver, les données à caractère personnel doivent être supprimées lorsqu'un recours n'est plus possible.

Il est donc important de décider quels documents ou données à caractère personnel sont pertinent(e)s pour faire office de preuves suffisantes. En pratique, cela peut se révéler difficile, mais un principe général sera établi et décrit dans le Registre de traitement, même s'il faut adapter le scénario au cas par cas, lors de la vérification du contenu d'une base de données.

Exemple

Lorsque TF BANK reçoit plusieurs candidatures pour un poste vacant. À moins qu'il n'existe une raison manifeste de les conserver, le service des Ressources Humaines ne doit pas conserver les dossiers de recrutement des candidats non recrutés plus longtemps que le délai légal au cours duquel un recours peut être introduit contre le processus de recrutement.

3.1.4 Exceptions

Il est possible de conserver des données à caractère personnel pendant plus longtemps :

- A des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique et historique ou à des fins statistiques ;
- Dans le but d'exercer ou de protéger son droit devant un tribunal (par exemple un conflit de travail).

À condition toutefois que la confidentialité de ces données soit toujours garantie. On considère, lors du traitement de données à des fins statistiques par exemple, que l'anonymisation ou la pseudonymisation des données apporte un niveau de protection suffisant aux intérêts des personnes concernées.

3.2. Archivage des données à caractère personnel

3.2.1. Un archivage sélectif

TF BANK, en tant que le responsable de traitement, doit veiller à archiver uniquement les données permettant de respecter l'obligation prévue par les normes commerciales et juridiques. Il doit opérer un tri parmi la totalité des données collectées pour ne garder que les seules données indispensables.

3.2.2. Le choix d'un mode d'archivage

TF BANK, en tant que le responsable de traitement, doit choisir un mode d'archivage.

Pour les archives intermédiaires, les données peuvent ainsi être archivées :

- dans une base d'archivage spécifique, distincte de la base de données active, avec des accès restreints aux seules personnes ayant un intérêt spécifique selon leurs fonctions. (par exemple, la création et l'archivage des données dans une GED pour que le DPO ait l'accès afin de répondre aux clients lors de la demande de l'exercice de droits).
- dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique pour les rendre inaccessible aux personnes n'ayant plus d'intérêt à les traiter. (par exemple, la réalisation du cloisonnement des données sur T24 pour que chaque département ait un statut différent d'accès).

Pour les archives définitives (par exemple, l'archivage des données dans l'intérêt public), il est recommandé de les conserver sur un support physique indépendant, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter.

3.2.3. Un archivage sécurisé

TF BANK, en tant que le responsable de traitement, doit également prévoir des mesures techniques et organisationnelles appropriées afin de protéger les données archivées. Ces mesures doivent assurer un niveau de sécurité approprié au regard des risques et de la nature de données. Par ailleurs, toutes les informations, soit elles sont archivées ou copiées sur un support de sauvegarde, soit sur les données actives, sont soumises au même niveau de protection.

Lorsque l'archivage est confié à un sous-traitant, TF BANK doit s'assurer que son prestataire présente des garanties suffisantes en matière de sécurité et la confidentialité des données qui lui sont confiées.

3.3. Suppression des données à caractère personnel

Un processus de purge, adapté aux normes commerciales et juridiques, doit être décrit dans le registre de traitement décrivant les principales caractéristiques de chaque application des bases de données contenant des données à caractère personnel.

3.3.1. Purge automatisée ou semi-automatisée

Idéalement, la meilleure pratique pour les applications ou bases de données contenant de grands volumes de données à caractère personnel est de programmer un processus automatisé de suppression des données dont le cycle de vie a atteint son terme, tel qu'il a été défini à l'origine.

Ce programme de purge peut :

- Soit faire partie du programme d'origine de l'application. Lorsqu'une nouvelle application est conçue, elle doit intégrer d'emblée une telle fonctionnalité (principe de la *confidentialité dès la conception*) ;
- Soit être un programme séparé qui est exécuté manuellement au moins une fois par an et qui supprime de la base de données toutes les données à caractère personnel ayant atteint leur « date de péremption ».

3.3.2. Purge manuelle

Si la base de données contenant les données à caractère personnel n'est pas structurée ou si l'application ne peut pas être repensée pour intégrer une fonction de purge automatique, alors le processus de suppression doit être effectué manuellement et régulièrement.

Prévoir une évaluation annuelle des données à caractère personnel contenues dans les applications et bases de données TF BANK, et supprimer tout ce qui n'est plus nécessaire est une bonne pratique.

Des audits seront programmés en accord avec le propriétaire de la base de données ou de l'application. Les constatations et les actions réalisées doivent être documentées (principe de la responsabilité) de manière à pouvoir être montrées à l'autorité de surveillance en cas de contrôle.

3.3.3. Alternatives techniques à l'effacement des données

Le RGPD prévoit certaines exceptions à l'obligation de suppression des données à caractère personnel.

TF BANK peut avoir des raisons de conserver des données à caractère personnel à des fins historiques, statistiques ou de recherche. Le RGPD prévoit que les données à caractère personnel conservées à ces fins peuvent être conservées indéfiniment tant qu'elles ne sont pas utilisées pour prendre des décisions affectant des individus, ou utilisées d'une manière susceptible de porter préjudice ou de susciter des difficultés.

Le traitement des données à caractère personnel à des fins historiques, statistiques ou de recherche doit faire l'objet de mesures de protection appropriées des droits et libertés de la personne concernée. Ces garanties doivent s'assurer que les mesures techniques et organisationnelles sont en place afin de respecter notamment le principe de minimisation des données.

Bien que le caractère sensible des données à caractère personnel diminue généralement avec le temps, une divulgation inappropriée de données vieilles de plusieurs décennies (p. ex. casiers judiciaires) peut encore avoir un effet extrêmement préjudiciable sur un individu. C'est pourquoi la sécurité des données qui ne peuvent pas être anonymisées est primordiale.

L'anonymisation ou la **pseudonymisation** des données à caractère personnel est considérée comme un moyen approprié de protéger les intérêts de la personne concernée, tant que cette technique ne permet plus d'identifier les personnes concernées.

- **L'anonymisation** est le processus consistant à modifier les données sous une forme qui ne nomme pas l'individu et sous laquelle il est peu probable qu'il soit identifié ;
- **La pseudonymisation** est le traitement de données de telle sorte que les données ne peuvent plus être attribuées à une personne concernée sans l'utilisation d'informations supplémentaires. Ces informations supplémentaires doivent être conservées séparément et faire l'objet de mesures techniques et organisationnelles appropriées.

La pseudonymisation exige d'établir un cadre de travail de mesures techniques et organisationnelles dédiées pour préserver la nature pseudonymique des données. Il convient de noter que le RGPD considère toujours les données pseudonymisées comme des données à caractère personnel : les données pseudonymes peuvent être réidentifiées dans certains cas précis et demeurent donc des données à caractère personnel.

La pseudonymisation est encouragée car elle aide à se conformer aux obligations, telles que l'obligation de sécurité des données ou bien la confidentialité dès la conception et par défaut.

Le propriétaire de l'application, le RSSI et le DPO doivent choisir ensemble la technique à adopter, au cas par cas.

3.4. Obligations d'information

Dans le cadre de la conservation des données, les personnes concernées doivent être informées de :

- La période de conservation ;

- Si aucune période de conservation ne peut être fournie, les critères utilisés pour déterminer cette période ;
- La nouvelle période de conservation si la finalité du traitement a changé après obtention des données à caractère personnel.

4. Contact

En cas de questions ou de doutes concernant la présente politique ou les exigences en matière de protection des données, veuillez contacter directement le DPO de TF BANK (dpo@tfbank.fr).

Annexe

Processus de gestion du cycle de vie des données

