

Politique de confidentialité à destination des utilisateurs de DPS

1. Objet de la présente Politique

La présente Politique de confidentialité a pour objet d'informer les utilisateurs internes et externes de la RATP (ci-après « vous » ou « les Utilisateurs ») des conditions dans lesquelles leurs données à caractère personnel sont collectées et traitées dans le cadre de l'utilisation de l'application DPS. Elle est établie conformément au Règlement (UE) 2016/679 du 27 avril 2016 (RGPD) et à la loi n°78-17 du 6 janvier 1978 modifiée.

2. Identité du Responsable de traitement

S'agissant de la collecte et du traitement de vos données personnelles, de votre information et de la mise en œuvre effective de vos droits, le Responsable du traitement de vos Données Personnelles est RATP Sûreté, Business Unit de la RATP (Régie Autonome des Transports Parisiens), établissement public à caractère industriel et commercial, dont l'adresse est située au 54, quai de la Rapée, 75599 Paris Cedex 12, immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro 775 663 438, TVA intracommunautaire n° FR 96 775 663 438.

3. Finalités des traitements et données traitées

Les traitements mis en œuvre dans le cadre de la gestion des demandes de sécurisation poursuivent trois finalités principales :

3.1. Gestion des identités et contrôle des accès aux systèmes d'information Sûreté (création/gestion/suppression de compte DPS)

- Réception et traitement des demandes d'accès ;
- Création et administration des comptes ;
- Gestion des droits d'accès ;
- Revues périodiques des accès et prévention des accès obsolètes ;
- Gestion des renouvellements ;
- Support applicatif et accompagnement utilisateurs.

Données traitées à des fins de gestion des identités et contrôle des accès aux systèmes d'information Sûreté :

Données d'identification

- Nom, prénom, signature de l'utilisateur ;
- Nom, prénom, signature du responsable de l'utilisateur ;
- Autres données d'identification liées au compte notamment : données d'habilitation (identifiant, profil utilisateur, Type de profil, libellé du profil).

Données de vie professionnelle (utilisateurs et responsables utilisateurs)

- Affectation ;
- Département/Direction d'appartenance ;
- Adresse e-mail professionnelle ;
- Téléphone fixe/portable ;

3.2. Recueil des demandes de prestations de sûreté dans l'outil DPS

Les opérations de traitement réalisées dans l'application DPS sont fondées sur deux finalités principales :

- Recueil et analyse des demandes émanant de l'exploitant, du gestionnaire d'infrastructure, des FSI, des municipalités, des préfectures et de la BRF ;
- Veille opérationnelle relative aux préconisations du CESCO, aux événements générant de l'affluence, aux retours des équipes SUR et exploitants.

Données traitées :

Données d'identification

- Nom ;
- Prénom ;

Données de vie professionnelle

- Affectation ;
- Département/Direction d'appartenance ;
- Téléphone fixe/portable ;

Les utilisateurs peuvent, dans les champs libres, saisir des informations qui ne sont pas nécessaires au traitement de leurs demandes. Ces données ne sont pas prises en compte par RATP Sûreté dans le cadre de la conception ou de l'instruction des dispositifs. Il est également rappelé aux utilisateurs de s'abstenir de communiquer toute donnée relevant des catégories particulières au sens du RGPD dans le cadre des demande de dispositif de sécurisation.

3.3. Gestion des dispositifs de sûreté dans l'outil GEODE

Finalités :

- Prise en compte des besoins de sûreté exprimés via DPS;
- Fourniture de réponses adaptées à partir des informations collectées ;
- Appui au dimensionnement des dispositifs de sûreté.

Données traitées :

- Identiques à celles listées au point 3.2

4. Bases légales des traitements

Les traitements reposent sur :

- L'exécution d'une mission d'intérêt public, relative à la sûreté des réseaux ;
- L'intérêt légitime de la RATP, notamment la gestion des accès aux SI de RATP Sûreté ;
- Les obligations légales, dont celles liées à la cybersécurité et à la traçabilité.

5. Destinataires des données

Les données sont strictement accessibles :

- Aux services habilités de RATP Sûreté intervenant dans la gestion des accès (PPS : Projets, Prospective et Support), de la gestion des dispositifs de sûreté (CCDS : Centre de Conception des Dispositifs de Sûreté);
- Aux services techniques support assurant la maintenance applicative de DPS et GEODE (PPS);
- Aux prestataires dûment autorisés, opérant dans un cadre contractuel incluant des obligations de confidentialité conformes aux exigences interne et au RGPD (YPOK).

6. Durées de conservation

Les durées de conservation applicables sont :

6.1. Gestion des identités et des accès

- Conservation en base active : les données sont conservées pendant toute la durée du besoin d'accès lorsque la fin des accès est signalée immédiatement ; à défaut, elles sont maintenues jusqu'à la revue suivante;
- Pas d'archivage intermédiaire ;

- Suppression du compte : le mois du départ si information transmise, sinon à la prochaine revue des comptes.

6.2. Recueil des demandes de sécurisation

- Durée de conservation : 54 mois glissants ;
- Purge automatique à l'issue de la période de conservation.

6.3. Gestion des dispositifs de sécurité

- Durée de conservation : 56 mois glissants ;
- Purge automatique à l'issue de la période de conservation.

7. Sécurité et confidentialité des données

7.1. Pour RATP Sûreté :

Il est mis en œuvre toutes les mesures techniques et organisationnelles nécessaires afin de garantir :

- La confidentialité et l'intégrité des données ;
- La protection contre l'accès non autorisé ;
- La limitation stricte des accès aux seuls personnels habilités ;
- Le respect des durées de conservation ;

7.2. En ce qui concerne la sous-traitance YPOK :

Engagement du sous-traitant : la société YPOK

Le portail de téléservice YGRC est propulsé et hébergé par la société YPOK SA, dont le siège social se situe au 9, rue des Halles, 75001 PARIS via son sous-traitant CLOUD TEMPLE.

La société YPOK, en sa qualité de prestataire hébergeur, de prestataire de maintenance, et de sous-traitant de RATP Sûreté, s'engage à :

- ne traiter les Données que sur instruction documentée de RATP Sûreté;
- veiller à ce que les personnes autorisées à traiter les Données s'engagent à respecter la confidentialité des Données, via une Charte d'éthique interne ;
- garantir le respect de l'obligation d'intégrité et de sécurité des Données et, dans la mesure des moyens technologiques disponibles, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès en :
 - prenant toute mesure permettant d'empêcher toute utilisation détournée, malveillante ou frauduleuse des Données,
 - limitant l'accès aux Données à un nombre limité de personnes spécialement habilitées à cet effet,
 - respectant son obligation de confidentialité, d'intégrité et de sécurité des Données à l'occasion des opérations de maintenance de la plateforme (l'ensemble des salariés de la société YPOK ayant signé une charte relative à l'utilisation des ressources technologiques),
 - effectuant un audit de sécurité externe annuel dont la conclusion sera accessible à RATP Sûreté;
- selon le choix de RATP Sûreté, supprimer toutes les Données ou les renvoyer à RATP Sûreté au terme de la prestation de maintenance, et détruire les copies de sauvegarde existantes, sous réserve d'une obligation légale de conservation des Données, auquel cas RATP Sûreté demandera que les Données et les copies de sauvegarde lui soient renvoyées.
- le cas échéant, aider RATP Sûreté, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées la saisissent en vue d'exercer leurs droits (droits d'accès, de rectification, d'effacement, d'opposition et de portabilité des Données), sachant que cette obligation doit être gérée en premier lieu par RATP Sûreté ;
- héberger les Données sur le territoire de la France métropolitaine pendant toute la durée du contrat.

La société YPOK s'interdit de :

- divulguer tout ou partie des Données à tout tiers non autorisé ;
- céder ou louer à un tiers tout ou partie des Données ;
- utiliser tout ou partie des Données à des fins professionnelles, personnelles ou privées autres que celles nécessaires à l'exécution d'une mission de maintenance ;
- copier ou stocker sous quelque forme que ce soit tout ou partie des Données pour une utilisation autre que celle d'assurer la maintenance du portail.

Conformité réglementaire et Audits

RATP Sûreté pourra réaliser des audits de conformité réglementaire en matière de traitement de Données, et ce au maximum une fois par période de douze (12) mois.

À la demande de RATP Sûreté, la société YPOK met à sa disposition les informations nécessaires pour démontrer le respect des obligations prévues au présent article, y compris des inspections, par RATP Sûreté ou un autre auditeur qu'elle a mandaté, et contribuer à ces audits.

La société YPOK informera RATP Sûreté si, selon elle, une instruction constitue une violation des dispositions réglementaires relatives à la protection des données.

8. Droits des personnes concernées

Vous disposez des droits suivants :

- **Droit d'accès :** Vous pouvez obtenir la confirmation que des données vous concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, en recevoir une copie ainsi que l'ensemble des informations prévues à l'article 15 du RGPD (finalités, catégories de données, destinataires, durée de conservation, etc.). Vous pouvez y accéder via le menu 'Mon profil', ou bien, si les informations vous paraissent incomplètes, demander une copie de toutes les données disponibles.
- **Droit de rectification :** Vous pouvez demander à tout moment la correction des données personnelles inexacts ou incomplètes vous concernant.
- **Droit à la limitation :** Vous pouvez demander la suspension temporaire du traitement lorsque vous contestez l'exactitude des données, lorsque le traitement apparaît illicite, lorsque les données ne sont plus nécessaires mais doivent être conservées pour l'exercice ou la défense de droits en justice, ou encore lorsque vous vous êtes opposé au traitement le temps d'en vérifier la légitimité.
- **Droit d'opposition selon les bases légales ;** en effet lorsque le traitement repose sur l'intérêt légitime ou sur une mission d'intérêt public, vous pouvez vous opposer, pour des raisons tenant à votre situation particulière, au traitement de vos données.
- **Droit d'effacement ou droit de suppression** lorsque applicable: Vous avez le droit de supprimer toutes vos données dans les meilleurs délais si le traitement est illégal ou la finalité du traitement a disparu.

Si vous estimez, après nous avoir contactés, que vos droits ne sont pas respectés ou que le traitement présente une non-conformité, vous pouvez saisir la Commission nationale de l'informatique et des libertés (CNIL) via :

[https://www.cnil.fr/fr/plaintes/Pour exercer vos droits, vous pouvez contacter : Délégué à la protection des données de la RATP, 54 quai de la Rapée, LAC LT73, 75599 Paris Cedex 12](https://www.cnil.fr/fr/plaintes/Pour_exercer_vos_droits_vous_pouvez_contacter_Délégué_à_la_protection_des_données_de_la_RATP_54_quai_de_la_Rapée_LAC_LT73_75599_Paris_Cedex_12_ou_à_l'adresse_de_courrier_électronique_protection-donnees@ratp.fr) ou à l'adresse de courrier électronique : protection-donnees@ratp.fr

9. Mise à jour de la présente politique

RATP Sûreté se réserve le droit de modifier à tout moment la présente Politique de confidentialité, afin de tenir compte des évolutions réglementaires, organisationnelles, techniques ou fonctionnelles de l'application DPS. Les Utilisateurs seront informés de toute mise à jour substantielle par les moyens de communication habituels.