Directorate-General for Security and Safety
Directorate for Safety, Access and Assistance
Access and Visitors Unit

European Parliament

Data protection notice
Accreditation - Passes and authorisations granting access to European Parliament's premises

RECORD UNDER REVISION

Regulation (EU) 2018/1725[1] (herein after "the Regulation") applies to the processing of personal data carried out by the European Parliament.
Further to Article 15 and Article 16 of this Regulation, the European Parliament provides the data subjects with the following information:

- The controller is the European Parliament and the entity responsible for the processing of your personal data is the Access and visitors Unit, represented by:
  Data controller: The Head of Unit
  SAFE.dataprotection@europarl.europa.eu

- Contact details of the Data Protection Officer at the European Parliament:
  Offices: ADENAUER 14T012, SPAAK 55A007, DE MADARIAGA -1 022 - Tel : + 352 4300 23595
  data-protection@europarl.europa.eu

- **Purpose** of the processing:
  The Directorate-General for Security and Safety at the European Parliament processes personal data requested from the Institution's Members, staff, contractors, visitors and internal/external partners for the following purposes:

  - Granting access to European Parliament's premises;
  - Controlling access to European Parliament's premises;
  - Investigating security incidents; conducting security inquiries and auxiliary investigations; evaluating threats and analysing risks.

  The purpose of this processing operation is the production and management of passes and other authorisations granting access to Parliament's buildings, parkings and restricted access areas. A pass is defined as a close-range visual identification document. All holders must have their pass with them at all times whilst on Parliament premises. Each type of pass or authorisation entitles the holder to a specific type of access. Passes issued by Parliament may only be used by the holder.

- The **legal basis** governing this processing operation of the Directorate-General for Security and Safety:
  - ✓ Article 5.1 a) and b) of the Regulation (EU) 2018/1725
  - ✓ EP Bureau Decision of 3 May 2004 (Rules on access badges) (as amended)
  - ✓ Rules governing passes and authorisations granting access to Parliament premises (signed by the Secretary-General on 13th December 2013)
  - ✓ Implementing provisions in respect of the rules governing passes granting access to Parliament premises (signed by the Director-General for Security and Safety on 25th November 2016)

[1] **Regulation (EU)** 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1543307408230&uri=CELEX:32018R1725

- ✓ Internal rules on Parking areas at the European Parliament (signed by the Secretary-General on 13th December 2013)
- ✓ Quaestors notice (01/2011) - Signing a safety book when entering the premises after 11:00 pm (PE 455.046/Quaest)
- ✓ EP Bureau Decision of 15 January 2018 - Rules governing Security and Safety in the European Parliament (2018/C79/04)

- The **categories** of personal data collected and used for the processing operation are:
  Depending on the pass/type of authorisation issued, the personal data collected may vary. The standard accreditation data collected data are:
  Family and first names, date of birth, nationality, type and reference number of an official identity document, photo and the validity of the pass or authorisation. As well as this, to facilitate the ability to invite visitors, the Access and Visitors Unit may collect data subjects' email address.

  Depending on the pass, some other data may be processed:
  T1 Members of the European Parliament: political group or aggregation
  T2 Member's entourage: Member related to, political group or aggregation
  T3 Officials and other servants of Parliament: personal number, status, start and end date of the contract, place of employment, office / building, office telephone number
  T4 Persons having a direct or indirect contractual link with Parliament (service providers):
  name external company (firm), nature of work / hours performed
  name and first name of the responsible official, telephone / GSM, e-mail, DG and service responsible for the contracts, dates of the contract
  T5 Media Representatives: represented entity
  T6 Members of the diplomatic corps and staff of international organisations and equivalent bodies: represented entity
  T7 Representatives of interest groups: representatives of interest groups seeking access rights to Parliament will be asked to provide additional personal information in accordance with the rules governing access to EP premises through the Transparency Register (see http://europa.eu/transparency-register/index_en.htm). An introductory letter, employment certificate and other documents showing the activity and status of the represented organisation may also be required (these documents are only consulted through the TR and not further processed by the Access and visitors Unit). After representatives' requests for accreditation are approved, their names and the period of validity of their badge will be published on the Transparency Register website.
  T8 Long-term visitors
  T9 Visitors: ID document expiry date is also collected. The official identity document presented by individual visitors may be scanned to extract such data or to confirm a visitor's identity (ID document is not kept nor further processed). For some visitors an email address will also be collected.

  Vehicles:
  Pass holders entitled to enter the parking, might send a request to the Access and visitors Unit with further personal data regarding their vehicle and the person entitled to use it. In order to issue a car pass, the following personal data is processed: email, plate number, country of registration, fuel, make, type, colour and RFID tag number.
  For service providers wishing to enter the parking, the following additional information should be provided: name external company (firm), name and first name of the responsible official and contract number.

  Some other personal data may be collected in order to grant access to Parliament premises. For example, agents may check the identity of any person wishing to enter or already present in Parliament, they can also record the entry to, and exit from Parliament premises of persons and vehicles (as well outside the normal opening times). As well as this, agents may conduct other necessary operations related to access control.

RECORD UNDER REVISION

Other information regarding the different access authorisations is also processed (access logs, specific access, activation of electronic locks by badging etc).

- Personal data processed in order to produce the different passes and access authorisations come from different **sources:**

    - direct (communicated directly by the data subject)
    - indirect (collected in the following systems: CODICT, EPextPro, JOUREG, AXS2EP, Transparency Register, OSCO, and VISSEM). The only data that the Access and visitors Unit will take from these systems are those necessary for processing, issuing and printing titles and other access authorisations.

- The **time limits** for storing the data are the following:
  Personal data concerning passes are kept for the **duration of the validity of the access pass/authorisation.** After the termination of the validity they are kept for 2 years (off-line) for possible investigation needs.
  Personal data relating to the access's history (when badging at the entrances to EP premises) is kept online for 4 months (extract from badges use). This can also be extended to 2 years (off-line) for possible investigation needs.
  Regarding visitor's personal data, this will be kept for the duration of the accreditation and that of service providers for the duration of the contract. The retention period after these validities will be one year (it can also be 2 years in case of investigations).
  Regarding other authorisations granting access, personal data will only be used to the purposes for which it was collected and will not be stored for longer than necessary for these purposes.

- The **recipients** of the data:
  The personal data regarding passes and other access authorisations may be communicated to the security and other staff of the Directorate-General for Security and Safety. In the event of an investigation, personal data may also be communicated to the other DGs and departments of the other European Institutions.
  When the accreditation of representatives of interest groups are approved, their names and the period of validity of their badge will be published on the Transparency Register website.
  For those who benefit from the re-imbursement system for public transport season tickets under the Mobility Policy, access log data will be transferred to DG INLO for the duration of the transport season ticket's validity. DG INLO is in charge of processing these refunds and managing the parking access quotas. This data is processed by DG INLO according to the terms detailed in record 401.

- **Data transfer**
  Your personal data will not be communicated to a third country or to an international organization.

- There is no automated individual decision-making or profiling in this data processing.

- You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of the Regulation (EU) 2018/1725, in particular the right to access and to rectify your personal data. Where applicable, you also have the right to erase, to restrict or to object to the processing. You can exercise your rights by contacting the Data Controller and obtain further information at SAFE.dataprotection@europarl.europa.eu or contact the European Parliament Data Protection Unit at data-protection@europarl.europa.eu. Data subjects also have the right to lodge a complaint with the European Data Protection Supervisor edps@edps.europa.eu

RECORD UNDER REVISION

Parlement européen

Déclaration concernant la protection des données
Accréditation - Différents titres et autorisations d'accès au Parlement européen

Le règlement (UE) 2018/1725[2] (ci-après « le règlement ») s'applique au traitement des données à caractère personnel effectué par le Parlement européen.
Conformément à l'article 15 et à l'article 16 du règlement, le Parlement européen fournit aux personnes concernées les informations suivantes:

- Le responsable du traitement est le Parlement européen et l'entité responsable de ce traitement des données est l'Unité Accès et Visiteurs, représentée par :
  Responsable du traitement : Le Chef d'Unité
  SAFE.dataprotection@europarl.europa.eu

- Le délégué à la protection des données au Parlement européen peut être contacté :
  Bureaux: ADENAUER 14T012, SPAAK 55A007, DE MADARIAGA -1 022
  Tél : + 352 4300 23595
  data-protection@europarl.europa.eu

- La **finalité** de ce traitement :
  La Direction générale de la sécurité et de la protection du Parlement européen traite les données à caractère personnel des députés, du personnel statutaire, des contractants, des visiteurs ainsi que des partenaires internes ou externes aux fins suivantes:
  - autoriser l'accès aux bâtiments du Parlement européen ;
  - contrôler l'accès aux bâtiments du Parlement européen ;
  - enquêter sur les incidents ; mener des enquêtes de sécurité et des investigations complémentaires ; évaluer les menaces et analyser les risques.

  La finalité de ce traitement est la production et gestion des titres d'accès et autres types d'autorisations d'entrée aux bâtiments, garages ainsi qu'aux locaux et zones d'accès restreint du Parlement européen. Le titre d'accès est défini comme un document d'identification visuelle de proximité. Tout titulaire doit être en possession de ce titre. À chaque type de titre d'accès est associée une autorisation d'accès spécifique. Les titres d'accès délivrés par le Parlement sont à usage strictement personnel.

- Les **bases juridiques** concernant ce traitement des données sont :
  - ✓ Article 5.1 a) et b) du règlement (UE) 2018/1725
  - ✓ Règles relatives aux laissez-passer consolidées par le Bureau 03/05/2004
  - ✓ Réglementation portant sur les titres et autorisations d'accès aux locaux du Parlement européen (signée par le Secrétaire général le 13/12/2013)
  - ✓ Modalités d'application du règlement portant sur les titres d'accès au Parlement européen (signées par le Directeur général de la Direction générale de la sécurité et de la protection le 25/11/2016)
  - ✓ Règlement intérieur relatif aux zones de stationnement du Parlement européen (signée par le Secrétaire général le 13/12/2013)
  - ✓ *Quaestors notice* (01/2011) relative à la signature du livret de sécurité (safety book) pour accéder aux bâtiments après 11:00 p.m (PE 455.046/Quaest)
  - ✓ Réglementation concernant la sécurité et la protection au Parlement européen, Décision du Bureau du Parlement européen du 15 janvier 2018 (2018/C 79/04)

RECORD UNDER REVISION

[2] **Règlement (UE)** 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1543307408230&uri=CELEX:32018R1725

- Les **catégories des données utilisées** sont:
  Selon le titre ou autorisation d'accès émise les données personnelles collectées peuvent varier.
  Les données personnelles qui sont toujours collectées:
  Nom, Prénom, Date de naissance, Nationalité, Numéro et type de pièce d'identité officielle, photo ainsi que la validité du titre ou l'autorisation d'accès. Pour faciliter la possibilité d'inviter des visiteurs, l'adresse électronique (e-mail) peut être aussi collectée.

  En fonction des titres d'accès, certaines autres données peuvent être traitées:
  T1 Membres du Parlement européen: Groupe politique ou agrégation
  T2 Entourage: Membre du Parlement européen, Groupe politique ou agrégation
  T3 Fonctionnaires et autres agents du Parlement: Matricule, Statut, Lieu de travail, bureau / bâtiment, numéro de téléphone du bureau
  T4 Personnes ayant un lien contractuel direct ou indirect avec le Parlement (prestataires de services): Nom de l'entreprise externe (entreprise), Nature du travail / heures effectuées Nom et prénom du fonctionnaire responsable, téléphone / GSM, e-mail, DG et service responsable des contrats, dates du contrat
  T5 Représentants des médias: entité représentée
  T6 Membres du corps diplomatique et personnel des organisations internationales et organes équivalents: entité représentée
  T7 Représentants des groupes d'intérêt: Les représentants des groupes d'intérêt souhaitant obtenir des droits d'accès au Parlement seront invités à fournir des informations personnelles supplémentaires conformément aux règles régissant l'accès aux locaux du PE via le Registre de Transparence (voir http://europa.eu/transparency-register/index_en.htm). Une lettre de présentation, un certificat de travail et d'autres documents indiquant l'activité et le statut de l'organisation représentée (ces documents ne sont consultés que par le Registre de transparence et ne sont pas traités ultérieurement par l'Unité d'accréditation). Une fois les demandes d'accréditation des représentants approuvées, leurs noms et la période de validité de leur badge seront publiés sur le site web du Registre de transparence.
  T8 Visiteurs de longue durée
  T9 Visiteurs: La date d'expiration du document d'identité est également collectée. Le document d'identité officiel présenté par les visiteurs individuels peut être scanné pour extraire ces données ou pour confirmer l'identité d'un visiteur (la pièce d'identité n'est pas conservée ni traitée ultérieurement). Pour certains visiteurs, l'adresse électronique (e-mail) sera également collectée.

  Véhicules :
  Les détenteurs de laissez-passer autorisés à accéder aux parking peuvent envoyer une demande à l'Unité d'accréditation avec d'autres données personnelles concernant leur véhicule et la personne autorisée à l'utiliser. Afin de délivrer l'autorisation pour les véhicules, les données personnelles suivantes sont traitées : Accès aux parkings: e-mail, Immatriculation, Pays d'origine, Marque, modèle, couleur du véhicule, type de carburant et numéro de l'étiquette RFID. Concernant les vignettes pour les prestataires de services, il faut aussi préciser le nom de la société externe, gestionnaire/fonctionnaire responsable du contrat au sein du PE et son numéro de contrat.

  Certaines autres données personnelles peuvent être collectées afin de permettre l'accès aux locaux du Parlement. Par exemple, les agents peuvent vérifier l'identité de toute personne souhaitant entrer ou déjà présente au Parlement, ils peuvent également enregistrer l'entrée et la sortie des locaux du Parlement de personnes et de véhicules (aussi en dehors des heures d'ouverture normales). De plus, les agents peuvent effectuer d'autres opérations nécessaires liées au contrôle d'accès.

RECORD UNDER REVISION

D'autres informations concernant les différentes autorisations d'accès sont également traitées (journaux d'accès, accès spécifiques, activation des serrures électroniques par badges, etc.).

- Les données à caractère personnel qui sont traitées afin d'émettre les différents titres et autorisations d'accès proviennent des différentes **sources**:

  - directes (communiquées directement par la personne concernée)
  - indirectes (collectées dans les suivants systèmes: CODICT, EPextPro, JOUREG, AXS2EP, Registre de transparence, OSCO, VISSEM). Les seules données que l'Unité accréditation prendra de ces systèmes sont celles nécessaires au traitement, l'émission et impression des titres et autorisations d'accès.

- La **période de rétention**:
  Les données personnelles concernant les titres d'accès sont conservées pendant la **durée de la validité du titre ou l'autorisation d'accès.** Après la fin de validité elles sont conservées 2 ans (off-line) pour d'éventuels besoins d'enquête.
  Les données relatives à l'historique d'accès (suite à l'action de badger dans les lecteurs aux entrées) aux bâtiments et locaux du PE sont conservées **4 mois** en ligne. Cela peut être aussi prolongé 2 ans (off-line) pour d'éventuels besoins d'enquête.
  La période de rétention pour les données concernant les **visiteurs** et celles des **prestataires de services** sera d'un an après leur visite / fin de contrat (elle peut aussi être 2 ans en cas d'enquêtes).
  En ce qui concerne les autres autorisations donnant accès, les données personnelles ne seront utilisées qu'aux fins pour lesquelles elles ont été collectées et ne seront pas conservées plus longtemps que nécessaire à ces fins.

- Les **destinataires des données** :
  Les données personnelles de toutes les personnes qui sont titulaires d'un titre d'accès au Parlement européen ou d'un autre type d'autorisation d'accès peuvent être communiquées au personnel de la Direction générale de la Sécurité et la Protection en ayant besoin de les connaître.
  En cas d'enquête, les données personnelles peuvent aussi être communiquées aux autres DG's et services des autres Institutions européennes.
  Quand les demandes d'accréditation des représentants des groupes d'intérêt sont approuvées, leurs noms et la période de validité de leur badge sont publiés sur le site web du Registre de transparence.
  Pour les personnes bénéficiant du système de remboursement des abonnements de transports publics mis en place dans le cadre de la Politique de Mobilité, les données de l'historique d'accès seront transférées à la DG INLO pour la durée de l'abonnement de transport. La DG INLO est chargé du traitement de ces remboursements et de la gestion des quotas d'accès au parking. Ces données sont traitées par la DG INLO selon les modalités détaillées dans le registre 401.

- **Transfert de données**
  Vos données à caractère personnel ne seront communiquées ni à un pays tiers, ni à une organisation internationale.

- Il n'existe pas de prise de décision individuelle automatisée, ni de profilage dans ce traitement de données.

- Vous bénéficiez des **droits** spécifiques en tant que « personne concernée » au titre du chapitre III (articles 14 à 25) du règlement (UE) 2018/1725, en particulier le droit d'accès et de rectification de vos données à caractère personnel. Le cas échéant, vous avez également le droit

RECORD UNDER REVISION

Parlement européen

d'effacer, de restreindre ou de vous opposer au traitement. Vous pouvez exercer vos droits en contactant le responsable du traitement et obtenir de plus amples informations SAFE.dataprotection@europarl.europa.eu ou contacter le unité de protection des données du Parlement européen data-protection@europarl.europa.eu. Les personnes concernées ont le droit de déposer une plainte auprès du contrôleur européen de la protection des données edps@edps.europa.eu.

RECORD UNDER REVISION