

1.1 MANDATORY INFORMATION

In accordance with article 32 of the amended law of January 6, 1978, we inform you that the personal data collected are under the responsibility of our president Mr. Gabriel Mitrache in his capacity as leader of the association. The personal data that we collect can be intended for the realization of the internal procedures (management of the membership, management of the payments of service...) but also related to the realization of our services such as the audits, the tests of intrusion and the audits of conformity with the personal data legislation.

The recipients of your personal data can be the secretary general, a project manager within ComEx or the DPO.

In accordance with the French Data Protection Act, you have the right to access, modify and object to your personal data for legitimate reasons. To exercise one of these rights, you can send your request to our DPO at dpo@appld-ee.eu. Our DPO undertakes to reply as quickly as possible, within a maximum of two months. Without a response from us, you can then submit your request to the CNIL.

1.2 PROCESSING OF REQUESTS FROM PERSONS CONCERNED (EXERCISE OF THEIR RIGHTS)

The serenity of our relationship with our members is essential. To do this, we do everything possible to inform our members of requests related to personal data. The European regulation reinforces and grants rights to the persons concerned.

We have decided to anticipate these requests by providing our members with a complete sheet explaining and reiterating their rights as well as the procedure to follow for any complaint or request.

1.3 DATA PRIVACY IMPACT ASSESSMENT

Personal data can be extremely diverse, all of which must be protected according to their level of criticality. To this end, the DPO conducts Data Privacy Impact Assessments (DPIA) on the most risky operations.

A working group led by the DPO will draw up a list of eight questions; these questions will help determine whether the processing requires an impact assessment. The first round of assessments will begin no later than February 1, 2021.

When the outcome of the questionnaire is positive, a complete analysis of the risks to the privacy of individuals is carried out by the DPO with the help of the operational staff concerned. The analysis is based in particular on the legal texts and the recommendations of the CNIL in terms of purpose, proportionality of processing, relevance of data, retention period and information to individuals.

If the processing is determined too risky for privacy, we shall cancel its implementation or develop an action plan with advanced technical security measures (anonymization, encryption ...).

The APPLD is committed to ensuring that the privacy of its members is protected as much as possible. In this sense, privacy protection is considered and evaluated at the design and inception stage of a project.

Regular compliance reviews are conducted to assure our members and partners of our high level of data protection.

Impact assessments are conducted annually under the direction of the DPO.

I.4 CNIL AUDITS

Although we make every effort to ensure a high level of compliance with legal obligations, we are not exempt from a CNIL audit. Thus, our DPO keeps a clear and up-to-date register of processing operations, which he can easily transmit to the CNIL experts.

I.5 DATA BREACH AND SECURITY LEAKS

We make every effort to maintain an excellent level of protection for our data systems. However, because perfect security does not exist, we are exposed to security breach threats. Therefore, in the event of a data breach, the DPO and the President have developed a specific breach management procedure.

First, the ExCom acts as quickly as possible to determine the cause and nature of the breach. They inform the DPO as soon as the breach is detected. The DPO, together with Comex, can establish a corrective action plan.

A data breach requires urgent, precise and rigorous action.

I.6 SUBCONTRACTING MANAGEMENT

In the event that personal data is processed by a subcontractor on behalf of APPLD, we will make every effort to ensure that the subcontractor provides sufficient guarantees for the protection of personal data.

A procedure for managing subcontracting has therefore been set up, according to the following guidelines.

First, the DPO systematically verifies that the contract proposed by the subcontractor meets the requirements of the GDPR. The contract must stipulate the nature and purpose of the processing, the object and duration of the data storage, as well as the type of personal data and the categories of data subjects.

Finally, the contract must provide for documentation and traceability; the security measures the processor implements, cooperation with authorities, assistance in handling requests from individuals in exercising their rights, notification of security breaches, the processor's recourse to another sub-processor, and the fate of the data at the end of the contract.



Gabriel Mitrache, President



Albert Lahoud, DPO

I.7 MENTIONS D'INFORMATIONS OBLIGATOIRES

Conformément à l'article 32 de la loi du 6 janvier 1978 modifiée, nous vous informons que les données personnelles recueillies sont sous la responsabilité de notre président M. Gabriel Mitrache en sa qualité de dirigeant de l'association. Les données personnelles que nous collectons peuvent être destinées à la réalisation des procédures internes (gestion des adhésions, gestion des paiements de prestation...), des services rendus mais également liées à la réalisation de nos prestations tels que les audits, les tests d'intrusion et les audits de conformité à la législation sur les données personnelles.

Les destinataires de vos données personnelles peuvent être ainsi, le secrétaire général, un responsable de projet au sein du ComEx ou bien le DPD.

Conformément à la Loi Informatique et Libertés vous disposez d'un droit d'accès, de modification et d'opposition sur motif légitime. Pour exercer l'un de ses droits, vous pouvez envoyer votre demande à notre DPD à l'adresse dpo@appld-ee.eu. Notre DPD s'engage à vous répondre le plus rapidement possible, dans un délai de deux mois maximum. Sans réponse de notre part vous pouvez alors réaliser votre demande auprès de la CNIL.

I.8 TRAITEMENT DES DEMANDES DES PERSONNES CONCERNEES (EXERCICE DE LEURS DROITS)

La sérénité de nos rapports avec nos membres est essentielle. Pour ce faire, nous faisons tout notre possible pour renseigner au mieux ces derniers notamment concernant leurs demandes liées aux données personnelles. La réglementation européenne conforte et accorde des droits aux personnes concernées. Nous avons décidé d'anticiper ces demandes en mettant à la disposition de nos membres une fiche complète expliquant et réitérant leurs droits ainsi que la procédure à suivre pour toute réclamation ou demande.

I.9 ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES

Les données personnelles peuvent être extrêmement diverses, toutes doivent être protégées selon leur niveau de criticité. Pour ce faire, le DPD réalise des analyses d'impact sur la vie privée (Data Privacy Impact Assessment - DPIA) sur les traitements les plus risqués.

Un groupe de travail piloté par le DPD élaborera une liste de 8 questions permettant de déterminer rapidement si le traitement nécessite ou non une étude d'impact. Le premier cycle d'évaluation débutera au plus tard le 1er février 2021.

Lorsque l'issue du questionnaire est positive, une analyse complète des risques pesant sur la vie privée des personnes est effectuée par le DPD à l'aide des opérationnels concernés. L'analyse s'appuie notamment sur les textes légaux et les recommandations de la CNIL en termes de finalité, de proportionnalité du traitement, de pertinence des données, de durée de conservation et de l'information des personnes.

Lorsque le traitement s'avère effectivement risqué pour la vie privée, nous annulons sa réalisation ou alors élaborons un plan d'action composé des mesures de sécurité techniques poussées (anonymisation, chiffrement...). L'APPLD tient à ce que la vie privée de ses membres soit la plus protégée possible. En ce sens, nous n'attendons pas le résultat des études d'impact pour agir. La protection de la vie privée est réfléchiée dès la conception d'une prestation.

Des examens de conformité réguliers sont réalisés afin de pouvoir assurer à nos membres et partenaires de notre haut niveau de protection des données personnelles.

Les analyses d'impact sont réalisées chaque année sous la direction du DPD.

I.10 CONTROLES DE LA CNIL

Bien que nous mettions tout en œuvre pour assurer un haut niveau de conformité aux obligations légales, nous ne sommes pas à l'abri d'un contrôle par CNIL. Ainsi, notre DPD tient un registre des traitements clair et à jour qui lui est facile de transmettre aux experts de la CNIL.

I.11 VIOLATION DES DONNEES ET FAILLES DE SECURITE

Nous mettons tout en œuvre pour maintenir un excellent niveau de protection de nos systèmes de données. Cependant parce que la sécurité parfaite n'existe pas, nous ne pouvons être infaillibles face aux menaces de violations de sécurité. Ainsi, en cas de violation de données, le DPD, et le président ont mis au point une procédure spécifique de gestion des violations.

Tout d'abord, le Comex agit le plus rapidement possible afin de déterminer la cause et la nature de la violation. Ils informent le DPD dès la détection de la violation afin que ce dernier établisse, avec le Comex, un plan d'actions correctives.

La violation des données suppose d'agir dans l'urgence et de manière précise et rigoureuse.

I.12 GESTION DE LA SOUS-TRAITANCE

Dans le cas où un traitement de données à caractère personnel est effectué par un sous-traitant pour le compte de l'APPLD, nous mettons tout en œuvre afin de s'assurer qu'il présente des garanties suffisantes en matière de protection des données personnelles. La procédure de gestion de la sous-traitance a ainsi été mise en place, selon le protocole suivant.

Dans un premier temps, le DPD vérifie systématiquement que le contrat proposé par le sous-traitant répond aux exigences du RGPD. Le contrat doit stipuler la nature et la finalité du traitement, l'objet et la durée de conservation des données, ainsi que le type de données à caractère personnel et les catégories de personnes concernées.

Enfin, le contrat doit prévoir la tenue de la documentation et la traçabilité, les mesures de sécurité que le sous-traitant met en place, la coopération avec les autorités, l'assistance dans le traitement des demandes des personnes dans le cadre de l'exercice de leurs droits, la notification des failles de sécurité, le recours du sous-traitant à un autre sous-traitant, et le sort des données à la fin du contrat.



Gabriel Mitrache, Président



Albert Lahoud, DPD