EUROPEAN DATA PROTECTION SUPERVISOR

Formulaire Web à remplir en cas de violation de données

Guide de l'utilisateur

Décembre 2018

TABLE DES MATIÈRES

1 Introduction

Le CEPD a déjà fourni aux institutions de l'UE les «*Lignes directrices concernant la notification des violations de données à caractère personnel à l'intention des institutions et organes européens*», qui contiennent des orientations spécifiques concernant l'obligation de notification prévue à l'article 34 du règlement (UE) 2018/1725.

Le CEPD offre deux possibilités aux responsables du traitement:

1. Remplir le formulaire en ligne[1] sur le site internet du CEPD: https://edps.europa.eu/form/personal-data-breach-notificatio_fr
2. Si la première option n'est pas disponible: télécharger un formulaire spécifique et le transmettre **sous forme cryptée**[2] directement à la boîte de messagerie fonctionnelle: data-breach-notification@edps.europa.eu

2 Objet

Le présent document a pour objet de fournir des instructions aux responsables du traitement sur la manière de remplir le formulaire Web relatif aux violations de données à caractère personnel, accessible sur le site internet du CEPD.

3 Lignes directrices relatives au formulaire Web

Le formulaire de notification de violation de données est subdivisé en deux sections:

SECTION A: Généralités

a) Dans cette section, vous devez saisir des informations générales concernant le type de notification, les coordonnées du responsable du traitement et celles du sous-traitant (le cas échéant).

[1] Actuellement disponible uniquement en anglais (EN). Le formulaire sera bientôt disponible en français (FR) et en allemand (DE).

[2] Le formulaire et les pièces jointes transmises par e-mail à la boîte de messagerie fonctionnelle data-breach-notification@edps.europa.eu doivent être cryptés (zip), et le mot de passe doit être communiqué au CEPD par d'autres moyens (par SMS ou par téléphone). L'institution de l'UE devra indiquer un numéro de téléphone dans son courriel afin que le CEPD puisse la joindre pour obtenir le mot de passe.

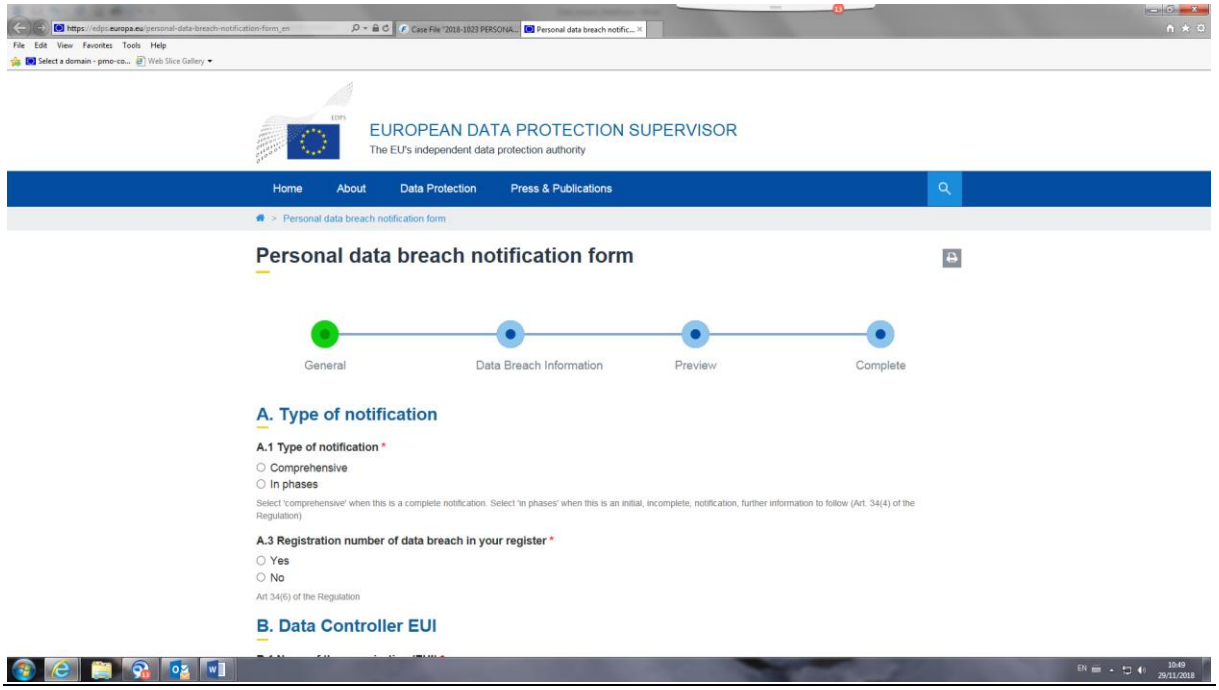

Figure 1 Formulaire à remplir en cas de violation de données à caractère personnel - Généralités

A. Type de notification

Dans cette section, vous devez choisir le type de notification de violation de données à caractère personnel:

«Notification complète», lorsqu'il s'agit d'une notification complète et que vous êtes en possession de toutes les informations disponibles concernant l'incident de violation de données à caractère personnel, ou

«Notification échelonnée» (article 34, paragraphe 4, du règlement 2018/1725), lorsque vous n'êtes pas en possession de toutes les informations disponibles concernant l'incident de violation de données à caractère personnel en raison du fait, par exemple, que l'enquête est toujours en cours et que vous soumettrez les informations ultérieurement de manière échelonnée.

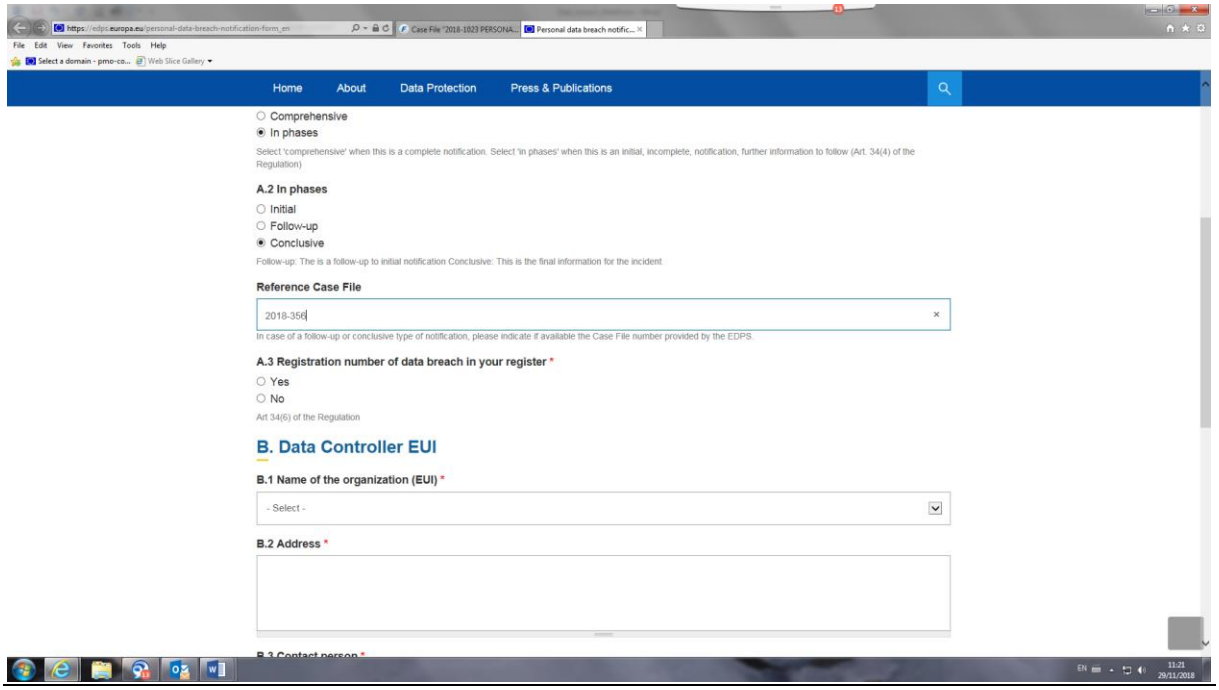

Figure 2 Notification échelonnée

A.2 Notification échelonnée

Si vous avez sélectionné «**Notification échelonnée**», une sélection supplémentaire apparaît et vous devez indiquer si la notification:

a) est la première notification, auquel cas vous devez sélectionner «**Notification initiale**»,

b) n'est ni la première ni la dernière notification, auquel cas vous devez sélectionner «**Notification de suivi**» et

c) est la dernière notification, auquel cas vous devez sélectionner «**Notification de clôture**»

Pour les options b) et c) ci-dessus, vous serez également invité à saisir le numéro du **Dossier de référence** si celui-ci vous a été communiqué lors de la première soumission. Il s'agit du numéro que le CEPD vous a communiqué par e-mail et dont le format est le suivant: *AAAA-numéro*, par exemple 2018-356.

A.3 Numéro d'enregistrement de la violation de données dans votre registre:

Conformément à l'article 34, paragraphe 6, du règlement 2018/1725, vous devez documenter toute violation de données à caractère personnel, y compris les faits la concernant, ses effets et les mesures prises pour y remédier.

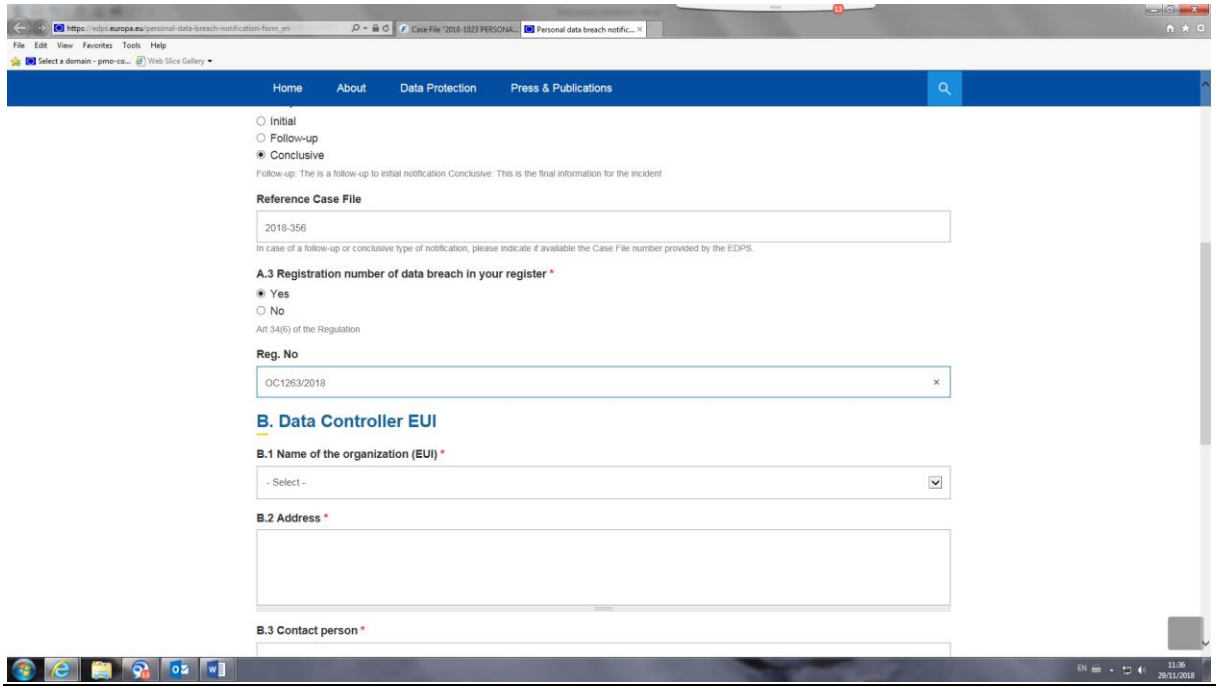

Figure 3 A.3 Numéro d'enregistrement

Si vous disposez d'un registre spécifique (registre interne du responsable du traitement) établi à cette fin, sélectionnez **Oui** et indiquez la référence spécifique de l'incident inscrite dans votre registre, le cas échéant *(p. ex. numéro, etc.)*.

B. Responsable du traitement de données EUI

Dans cette section, tous les champs marqués d'un astérisque (*) doivent obligatoirement être remplis.

B.1 Nom de l'organisation (EUI): sélectionnez le nom de votre organisation dans la liste déroulante ou **Autre** si son nom n'apparaît pas dans la liste, et saisissez manuellement le nom de votre organisation dans le champ **Veuillez préciser:** .

B.2 Adresse: indiquez l'adresse complète de votre organisation, y compris le nom de la rue, le numéro, le code postal, la ville et le pays.

B.3 Personne à contacter, B.4 Téléphone, B.5 Adresse e-mail: saisissez le nom, le numéro de téléphone et l'adresse e-mail de la personne à contacter pour les communications ultérieures avec le CEPD concernant ce dossier. Veuillez noter que le CEPD utilisera cette adresse e-mail pour vous envoyer l'accusé de réception une fois le formulaire soumis.

B.6 Délégué à la protection des données, B.7 Téléphone, B.8 Adresse e-mail: saisissez le nom, le numéro de téléphone et l'adresse e-mail du délégué à la protection des données de votre organisation.

C. Sous-traitant EUI

Cette section est facultative et ne doit être remplie que dans les cas où une violation de données à caractère personnel s'est produite dans le cadre des activités de traitement de votre sous-traitant (article 34, paragraphe 2, du règlement 2018/1725) et a également été notifiée par le sous-traitant.

Le cas échéant, *cochez la case*: «**Indiquez si la violation de données a été signalée par le sous-traitant**»

Les champs suivants seront activés et devront obligatoirement être remplis:

C.1 Nom de l'organisation: saisissez manuellement le nom de l'organisation du sous-traitant.

C.2 Adresse: indiquez l'adresse complète du sous-traitant, y compris le nom de la rue, le numéro, le code postal, la ville et le pays.

C.3 Personne à contacter, C.4 Téléphone, C.5 Adresse e-mail: saisissez le nom, le numéro de téléphone et l'adresse e-mail de votre sous-traitant pour les communications ultérieures avec le CEPD concernant ce dossier.

C.6 Délégué à la protection des données, C.7 Téléphone, C.8 Adresse e-mail: saisissez le nom, le numéro de téléphone et l'adresse e-mail du délégué à la protection des données du sous-traitant.

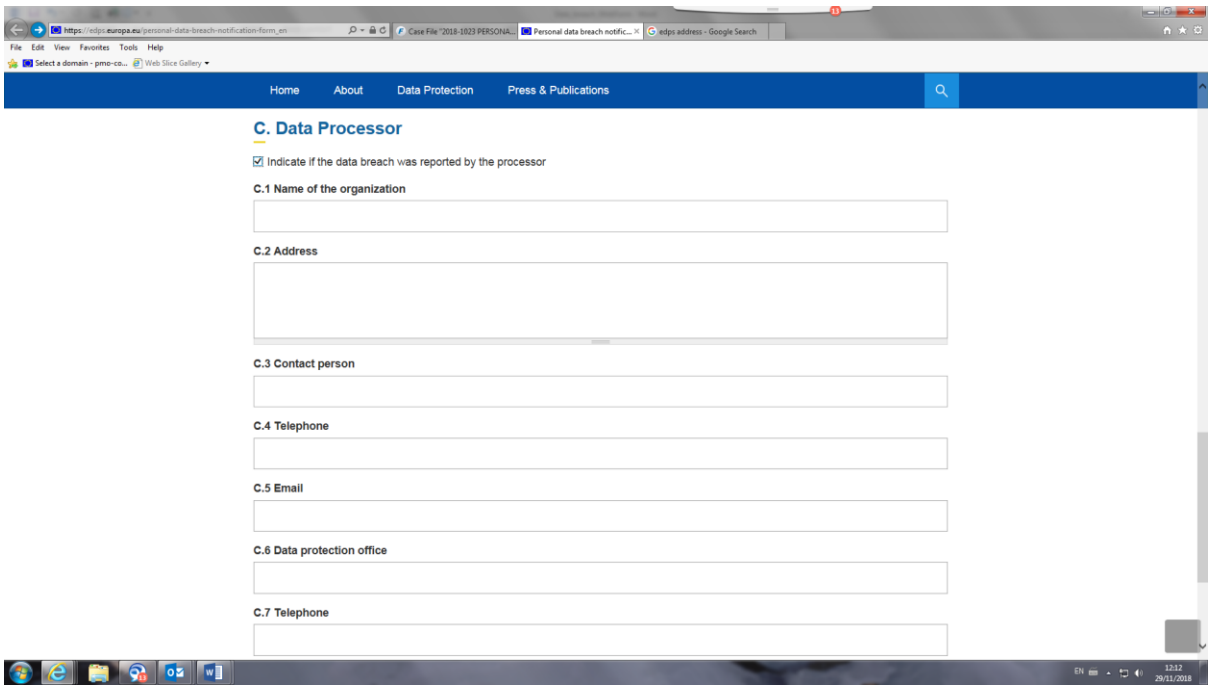

Figure 4 Sous-traitant

À la fin de la page, appuyez sur SUIVANT pour passer à la deuxième section de la notification.

SECTION II: Informations relatives à la violation de données

Dans cette section, vous devez fournir les principaux renseignements concernant l'incident de violation de données à caractère personnel, comme l'exigent les articles 34 et 35 du règlement. Certains champs de cette section ne sont pas obligatoires et vous pouvez remplir cette partie de la notification avec les informations dont vous disposez.

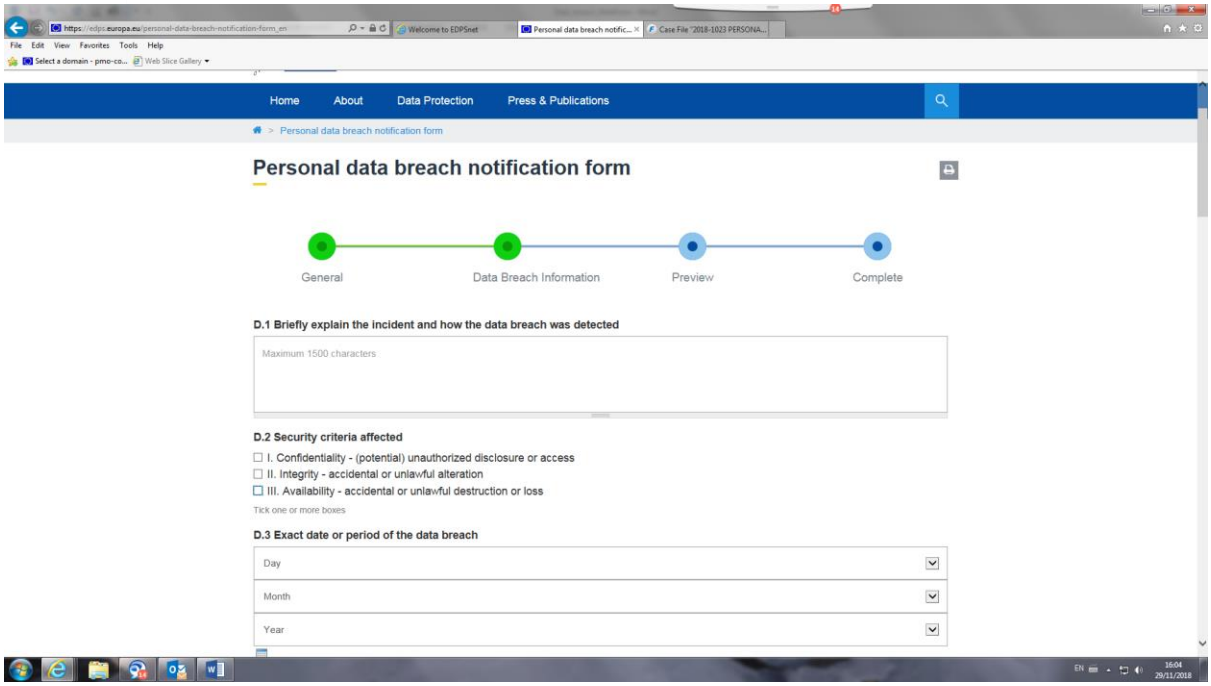

Figure 5 Section II: Communication d'une violation de données (1)

D.1 Expliquez brièvement l'incident et comment la violation de données a été détectée: indiquez dans la zone de texte libre (1 500 caractères maximum) la nature, les caractéristiques et les effets de l'incident de violation de données à caractère personnel et comment il a été détecté.

D.2 Critères de sécurité affectés: sélectionnez **un ou plusieurs** des trois types de critères de sécurité qui ont été affectés par l'incident de violation de données à caractère personnel: a) I. **Confidentialité** - lorsqu'il s'agit d'une divulgation ou d'un accès non autorisé à des informations personnelles, b) II. **Intégrité** - lorsqu'il s'agit d'une altération accidentelle ou illicite d'informations personnelles et c) III. **Disponibilité** - lorsque la destruction accidentelle ou illicite ou la perte d'informations personnelles est évidente.

D.3 Date ou période exacte de la violation de données: indiquez la date exacte en sélectionnant les valeurs correctes de la violation de données à caractère personnel ou, si vous ne connaissez pas la date exacte, utilisez le champ suivant pour saisir la période de la violation de données à caractère personnel ou toute autre information.

D.4 Date de détection: saisissez la date et l'heure exactes (indiquez votre heure locale) auxquelles vous avez pris connaissance de la violation de données à caractère personnel en sélectionnant les valeurs correctes dans les cases correspondantes.

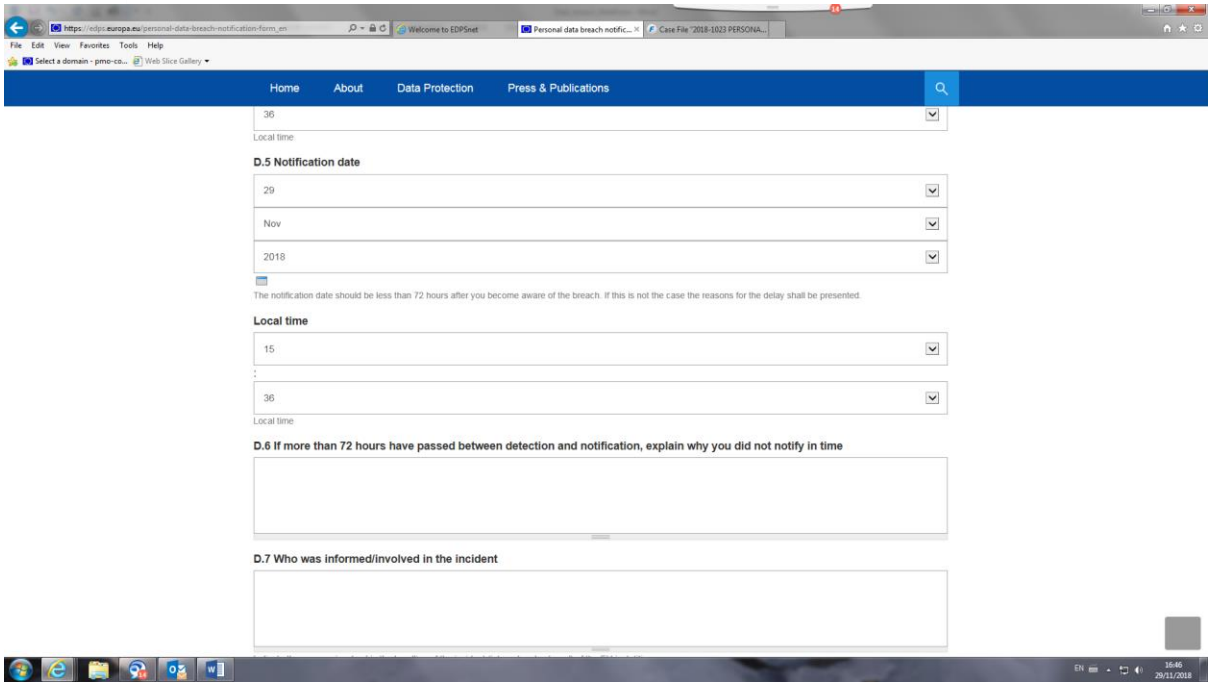

Figure 6 Communication d'une violation de données (2)

D.5 Date de notification: assurez-vous que la date et l'heure actuelles, qui sont remplies automatiquement dans le formulaire à titre indicatif, sont correctes (indiquez votre heure locale) concernant votre notification. En cas d'erreur, apportez les corrections nécessaires.

D.6 Si plus de 72 heures se sont écoulées entre la détection et la notification de la violation de données, expliquez pourquoi vous ne l'avez pas notifiée dans les délais: si vous avez notifié la violation de données avec plus de 72 heures de retard, expliquez les motifs du retard.

D.7 Qui a été informé/impliqué dans l'incident: indiquez les personnes qui sont ou ont été impliquées dans le traitement de l'incident (interne et externe) de l'institution de l'UE. Veillez à fournir des informations complètes.

D.8 Catégories de données à caractère personnel affectées: expliquez et énumérez tous les éléments/types de données qui ont été compromis, p. ex. nom et prénom, date de naissance, données financières, données sur la santé, etc.

D.9 Nombre approximatif de données à caractère personnel affectées: sélectionnez la valeur correcte et, si possible, précisez le nombre exact de données à caractère personnel qui ont été affectées par la violation.

D.10 Catégorie de personnes affectées: indiquez les catégories de personnes affectées par la violation, p. ex. personnel de l'UE, députés européens, citoyens européens, enfants, groupes vulnérables tels que les personnes handicapées, etc.

D.11 Nombre approximatif de personnes affectées: si possible, indiquez un chiffre pour chaque catégorie de personnes affectées, p. ex. 150 députés européens, 2 000 citoyens européens, 10 enfants, etc.

D.12 Conséquences probables ou réelles de la violation de données pour les personnes concernées: précisez si vous connaissez déjà les conséquences réelles ou probables de la violation de données à caractère personnel pour les personnes concernées. La violation de données peut entraîner des dommages physiques, matériels ou moraux pour les personnes concernées.

D.13 Estimation du risque pour les droits et libertés des personnes physiques: veuillez également sélectionner l'importance du risque: **Aucun risque, Risque, Risque élevé**

D.14 Expliquez brièvement comment l'évaluation du risque pour les droits et libertés des personnes physiques a été effectuée: précisez comment vous avez évalué le niveau de risque de la violation de données à caractère personnel, en indiquant si vous avez utilisé une méthode particulière.

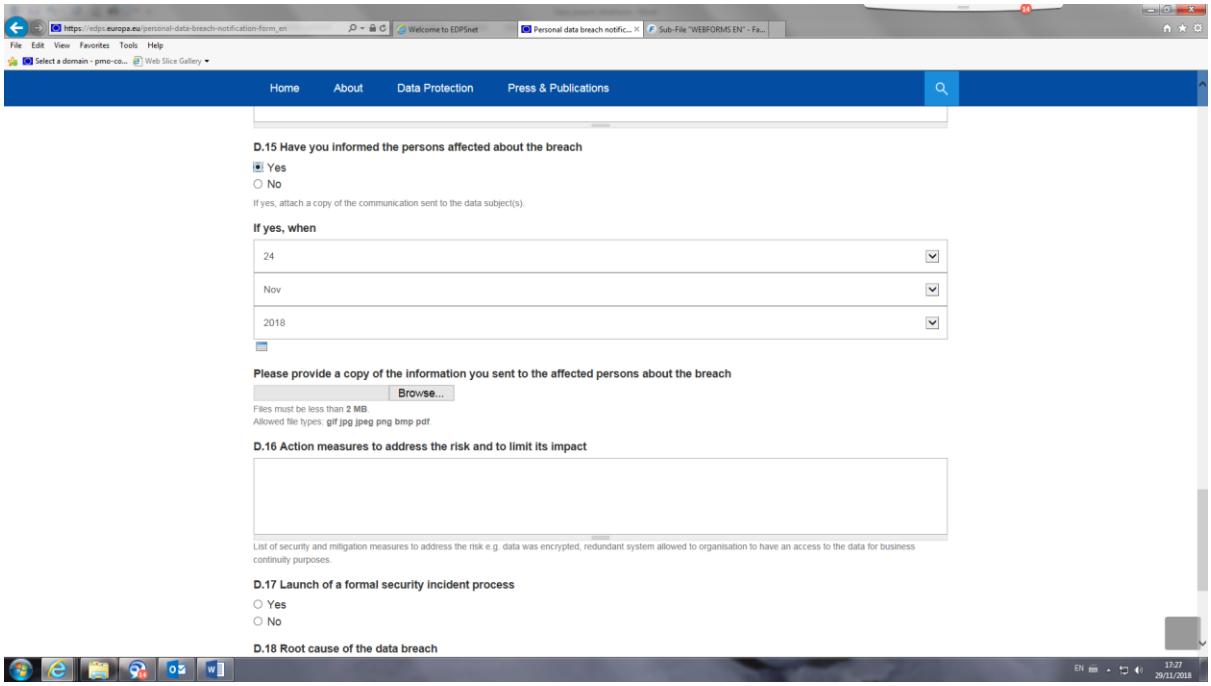

Figure 7 Information des personnes physiques

D.15 Avez-vous informé les personnes concernées de la violation? Sélectionnez **Oui** si vous avez déjà informé les personnes et ajoutez la date à laquelle vous avez envoyé ces informations, et veillez également à **joindre le fichier** contenant la notification aux personnes concernées.

Sélectionnez **Non** si vous n'avez pas informé les personnes concernées et précisez dans la zone de texte les raisons pour lesquelles vous ne l'avez pas encore fait.

D.16 Mesures prises pour gérer le risque et en limiter l'impact: expliquez brièvement si vous avez pris des mesures de sécurité et d'atténuation du risque, p. ex. si les données ont été cryptées, si un système redondant a été autorisé afin que l'organisation puisse avoir accès aux données à des fins de continuité des activités.

D.17 Lancement d'un processus officiel relatif à un incident de sécurité: sélectionnez **Oui** si un processus officiel relatif à un incident de sécurité a été lancé. Sélectionnez **Non** si aucun processus de ce type n'a été lancé et expliquez les raisons.

D.18 Cause première de la violation de données: expliquez la cause première de l'incident de sécurité ayant mené à la violation de données.

Une fois les deux sections remplies, vous pouvez soit appuyer sur PRÉCÉDENT et revenir à l'écran précédent, soit appuyer sur APERÇU pour vérifier les informations que vous avez saisies.

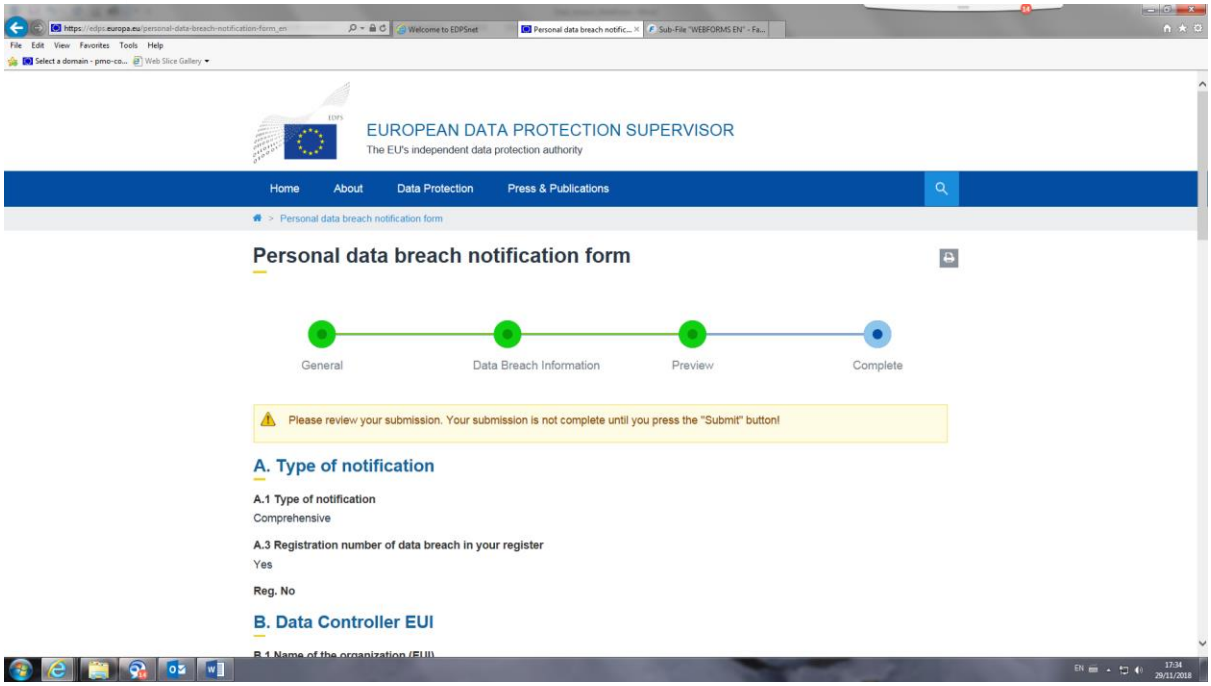

Figure 8 Aperçu de la notification

Après avoir vérifié le formulaire, cliquez sur **SOUMETTRE** au bas de la page pour soumettre le formulaire au CEPD.

Vous recevrez le message suivant:

MESSAGE

Nous vous remercions d'avoir soumis une notification de violation de données.

Vous recevrez un accusé de réception par e-mail dans les prochains jours, avec un numéro de référence de dossier que vous devrez utiliser dans vos communications ultérieures avec le CEPD.

Si vous ne recevez pas d'e-mail, veuillez nous contacter à l'adresse suivante: data-breach-notification@edps.europa.eu

Le CEPD vous enverra sous quelques jours un message de confirmation avec un numéro de référence de dossier spécifique pour votre notification que vous devrez utiliser dans toute communication ultérieure.