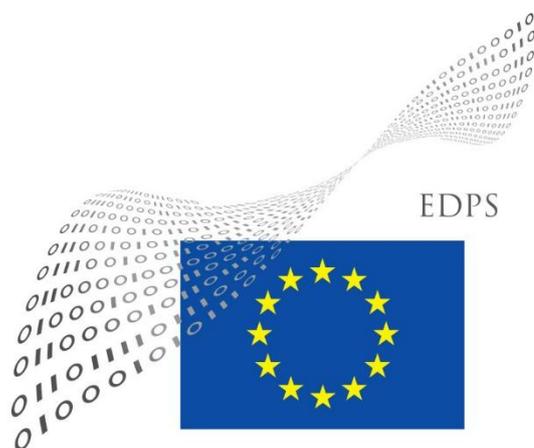


EUROPEAN DATA PROTECTION SUPERVISOR

Internetformular zur Meldung von Datenschutzverletzungen Benutzerleitfaden



Dezember 2018



INHALTSVERZEICHNIS

1	Einleitung	3
2	Zweck	3
3	Leitlinien zum Ausfüllen des Internetformulars	3

1 Einleitung

Der EDSB hat den Organen und Einrichtungen der EU bereits Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten (*Guidelines on personal data breach notification for the European institutions and bodies*) an die Hand gegeben, in denen spezifische Vorgaben für die Meldepflicht nach Artikel 34 der Verordnung (EU) 2018/1725 festgelegt sind.

Der EDSB bietet den für die Verarbeitung Verantwortlichen zwei Möglichkeiten:

1. Ausfüllen des Online-Formulars¹ auf der Website des EDSB unter: https://edps.europa.eu/form/personal-data-breach-notification_de
2. Wenn die vorstehend genannte Option nicht in Frage kommt, kann alternativ auch ein spezielles Formular heruntergeladen und **verschlüsselt**² direkt an die funktionale Mailbox gesendet werden:
data-breach-notification@edps.europa.eu

2 Zweck

Dieses Dokument enthält Hinweise, die die Verantwortlichen beim Ausfüllen des auf der EDSB-Website abrufbaren Internetformulars (WebForm) zur Meldung von Verletzungen des Schutzes personenbezogener Daten unterstützen sollen.

3 Leitlinien zum Ausfüllen des Internetformulars

Das Formular zur Meldung von Datenschutzverletzungen ist in zwei Abschnitte unterteilt:

ABSCHNITT A: Allgemeines

a) Dieser Abschnitt enthält allgemeine Angaben zur Art der Meldung sowie Informationen zur Identifizierung des Verantwortlichen und des Auftragsverarbeiters (sofern zutreffend).

¹ Das Formular ist aktuell nur auf Englisch (EN) verfügbar. Es wird jedoch in Kürze auch auf Französisch (FR) und Deutsch (DE) abrufbar sein.

² Ein per E-Mail an die funktionale Mailbox (data-breach-notification@edps.europa.eu) gesendetes Formular muss samt allen zugehörigen Anhängen verschlüsselt (ZIP-Datei) und mit einem Passwort versehen werden, das dem EDSB über einen anderen Kanal (per SMS oder Anruf) mitzuteilen ist. Das betreffende EU-Organ muss in der E-Mail eine separate Telefonnummer angeben, unter der der EDSB das Passwort anfordern kann.

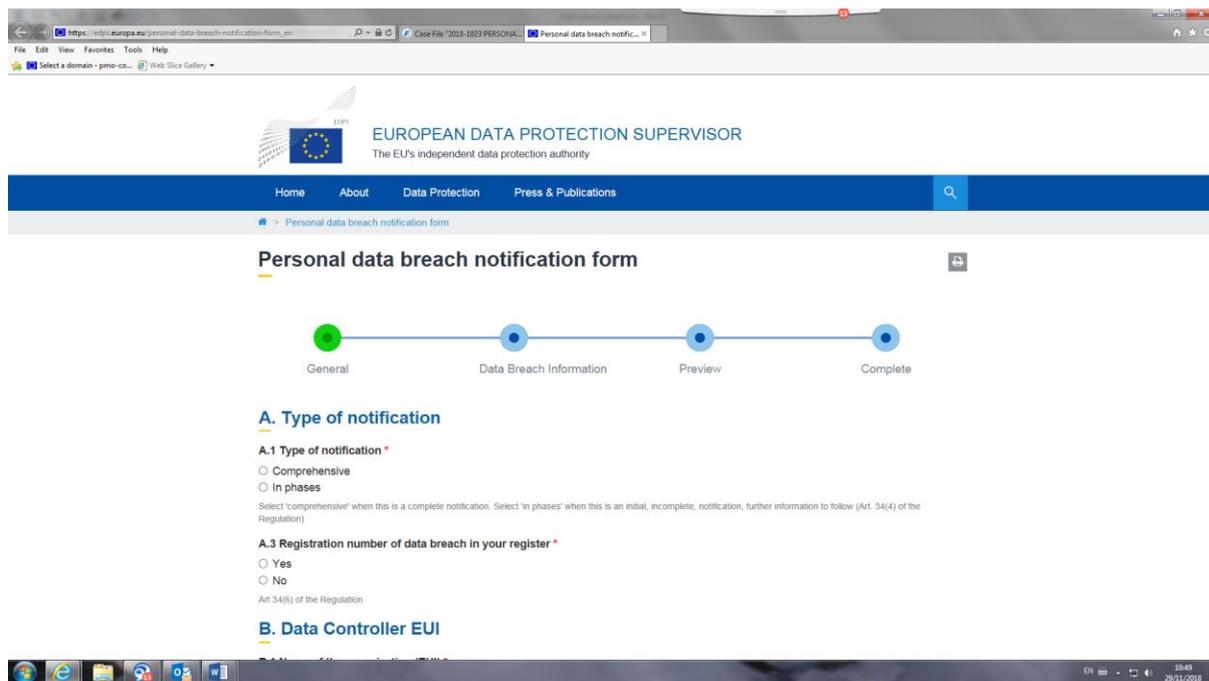


Abb. 1: Formular zur Meldung von Verletzungen des Schutzes personenbezogener Daten – Abschnitt „Allgemeines“

A. Art der Meldung

In diesem Abschnitt geben Sie an, um welche Art der Meldung bezüglich einer Verletzung des Schutzes personenbezogener Daten es sich handelt. Wählen Sie:

„Vollständig“, wenn es sich um eine vollständige Meldung handelt und Ihnen alle verfügbaren Informationen bezüglich der Verletzung des Schutzes personenbezogener Daten vorliegen, oder

„Schrittweise“ (vgl. Artikel 34 Absatz 4 der Verordnung (EU) 2018/1725), wenn Sie nicht über alle Informationen bezüglich der Verletzung des Schutzes personenbezogener Daten verfügen, weil beispielsweise der Vorfall aktuell noch untersucht wird, und Sie die erforderlichen Informationen nach und nach übermitteln werden.

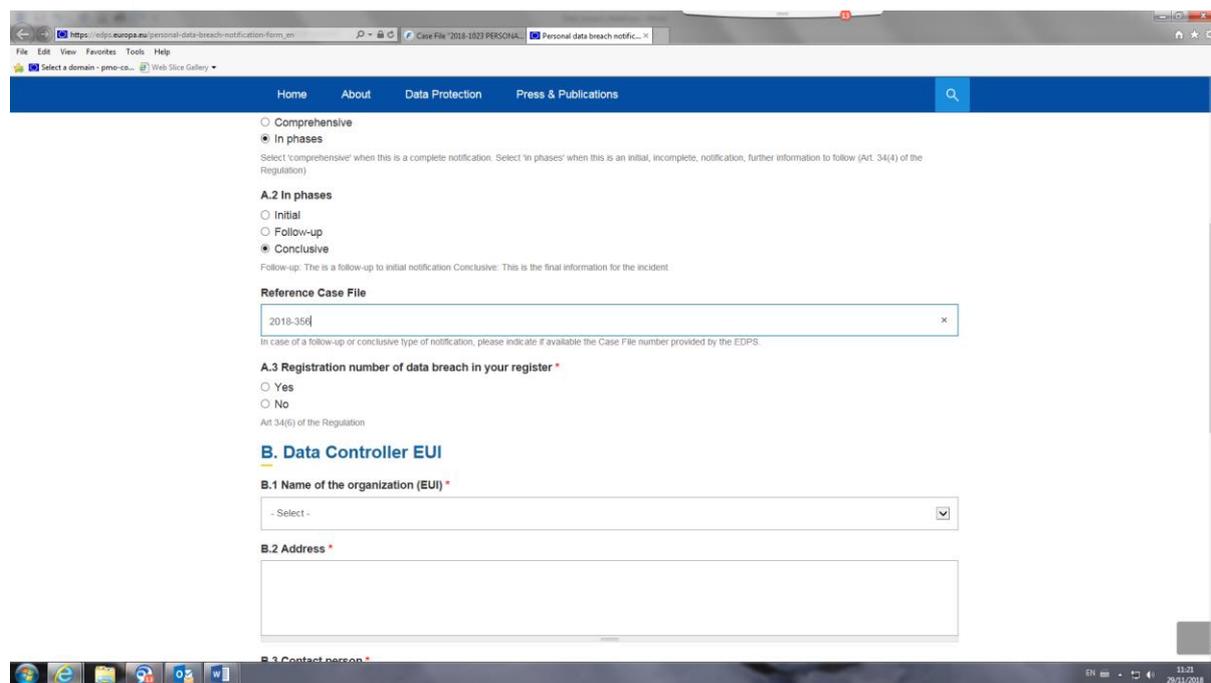
A screenshot of a web browser displaying the EDPS notification form. The browser's address bar shows 'https://edps.europa.eu/personal-data-breach-notification-form_en'. The page has a blue header with navigation links: Home, About, Data Protection, and Press & Publications. The main content area is titled 'Personal data breach notification form' and includes several sections: 'Comprehensive' (unselected), 'In phases' (selected), 'A.2 In phases' (with sub-options 'Initial', 'Follow-up', and 'Conclusive', where 'Conclusive' is selected), 'Reference Case File' (with a text input field containing '2018-356'), 'A.3 Registration number of data breach in your register' (with 'Yes' and 'No' options), and 'B. Data Controller EU' (with sub-sections 'B.1 Name of the organization (EU)' and 'B.2 Address'). The browser's taskbar at the bottom shows various application icons and the system clock indicating 13:21 on 20/11/2018.

Abb. 2: Schrittweise Meldung

A.2 Schrittweise

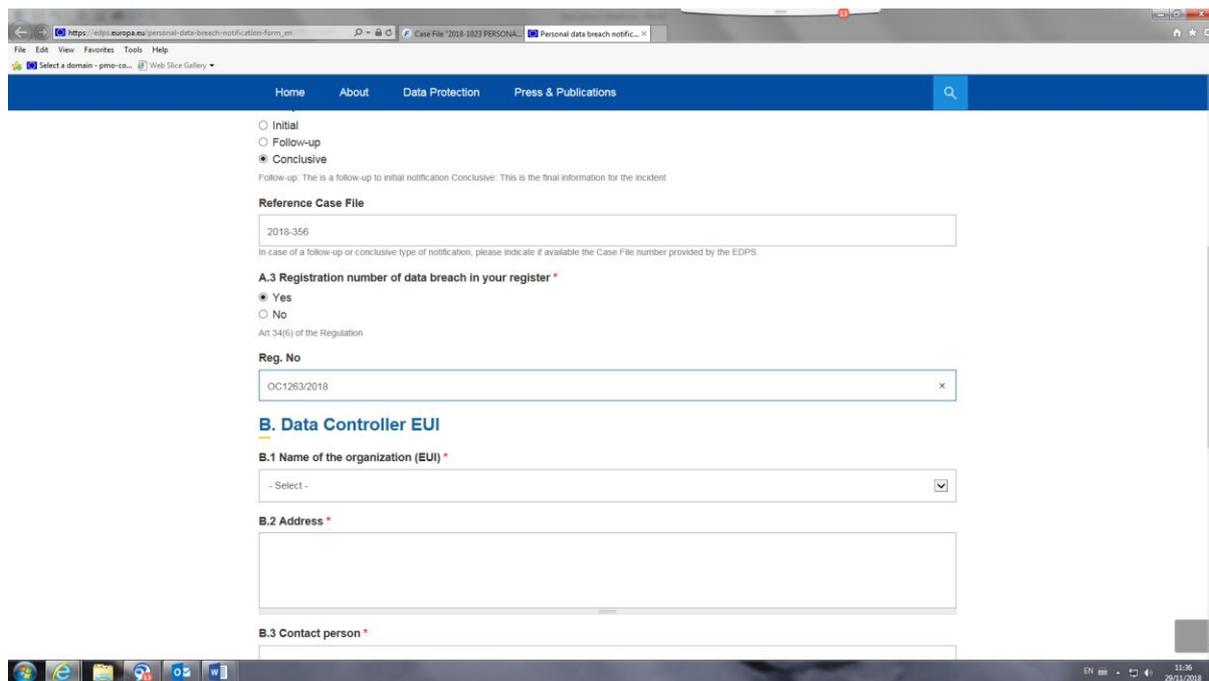
Wenn Sie bei der Art der Meldung die Option „**Schrittweise**“ gewählt haben, wird Ihnen ein weiteres Auswahlmenü angezeigt. Hier müssen Sie angeben, ob es sich bei der Meldung

- um die erste Meldung handelt – in diesem Fall müssen Sie „**Erstmeldung**“ wählen;
- nicht um die erste, aber auch nicht um die letzte (abschließende) Meldung handelt – in diesem Fall wählen Sie „**Folgemeldung**“; oder
- um die abschließende Meldung handelt – in diesem Fall müssen Sie „**Abschlussmeldung**“ wählen.

Wenn Sie Option b oder c gewählt haben, werden Sie aufgefordert, zusätzlich auch das **Aktenzeichen** anzugeben, wenn Ihnen dieses aus der Erstmeldung bekannt ist. Diese Nummer, die der EDSB Ihnen per E-Mail mitgeteilt hat, hat folgendes Format: *JJJJ-Nummer*, z. B. 2018-356.

A.3 Registrierungsnummer der Datenschutzverletzung in Ihrem Register:

Gemäß Artikel 34 Absatz 6 der Verordnung (EU) 2018/1725 müssen Sie jede Verletzung des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen dokumentieren.



The screenshot shows the 'Personal data breach notification form' on the EDPS website. The form is in the 'Conclusive' stage. It includes a 'Reference Case File' field with the value '2018-356'. Under section 'A.3 Registration number of data breach in your register', the 'Yes' option is selected, and the 'Reg. No' field contains 'OC1263/2018'. Section 'B. Data Controller EU' includes fields for 'B.1 Name of the organization (EU)', 'B.2 Address', and 'B.3 Contact person', all of which are currently empty.

Abb. 3: A.3 Registrierungsnummer

Wenn Sie über ein eigens zu diesem Zweck eingerichtetes Register verfügen (internes Register des Verantwortlichen), wählen Sie **Ja**, und geben Sie (sofern vorhanden) die genaue Referenz (z. B. *die Nummer*) des Vorfalls aus Ihrem Register an.

B. Verantwortlicher (EU-Organ)

In diesem Abschnitt sind alle Felder mit (*) obligatorisch und müssen ausgefüllt werden.

B.1 Name der Organisation (EU-Organ): Bitte wählen Sie Ihre Organisation aus der Auswahlliste aus oder wählen Sie den Eintrag **Sonstige**, wenn Ihre Organisation nicht in der Liste enthalten ist. In diesem Fall müssen Sie den Namen der Organisation im Feld **Bitte angeben**: manuell eintragen.

B.2 Anschrift: Bitte geben Sie die vollständige Anschrift Ihrer Organisation an, einschließlich Straße, Hausnummer, Postleitzahl, Stadt und Land.

B.3 Ansprechpartner, B.4 Telefon, B.5 E-Mail: Geben Sie den Namen, die Telefonnummer und die E-Mail-Adresse des Ansprechpartners an, über den die künftige Kommunikation mit dem EDSB in diesem konkreten Fall stattfinden wird. Bitte beachten Sie, dass der EDSB diese E-Mail-Adresse zur Versendung der Bestätigungsmail am Ende der Informationsübertragung verwendet.

B.6 Datenschutzbeauftragter, B.7 Telefon, B.8 E-Mail: Geben Sie den Namen, die Telefonnummer und die E-Mail-Adresse des Datenschutzbeauftragten Ihrer Organisation an.

C. Auftragsverarbeiter (EU-Organ)

Dieser Abschnitt ist optional und muss nur in Fällen ausgefüllt werden, in denen eine Verletzung des Schutzes personenbezogener Daten im Rahmen der Datenverarbeitungstätigkeit des Auftragsverarbeiters aufgetreten ist (Artikel 34 Absatz 2 der Verordnung (EU) 2018/1725) und diese auch vom Auftragsverarbeiter gemeldet wurde.

Falls dies zutrifft, kreuzen Sie bitte das folgende Kästchen an: **Die Datenschutzverletzung wurde vom Auftragsverarbeiter gemeldet.**

Die folgenden Felder werden daraufhin aktiviert und müssen ausgefüllt werden:

C.1 Name der Organisation: Bitte geben Sie manuell den Namen der verarbeitenden Organisation an.

C.2 Anschrift: Bitte geben Sie die vollständige Anschrift der verarbeitenden Organisation an, einschließlich Straße, Hausnummer, Postleitzahl, Stadt und Land.

C.3 Ansprechpartner, C.4 Telefon, C.5 E-Mail: Geben Sie den Namen, die Telefonnummer und die E-Mail-Adresse des Ansprechpartners in der verarbeitenden Organisation an, über den die künftige Kommunikation mit dem EDSB in diesem konkreten Fall stattfinden wird.

C.6 Datenschutzbeauftragter, C.7 Telefon, C.8 E-Mail: Geben Sie den Namen, die Telefonnummer und die E-Mail-Adresse des Datenschutzbeauftragten in der verarbeitenden Organisation an.

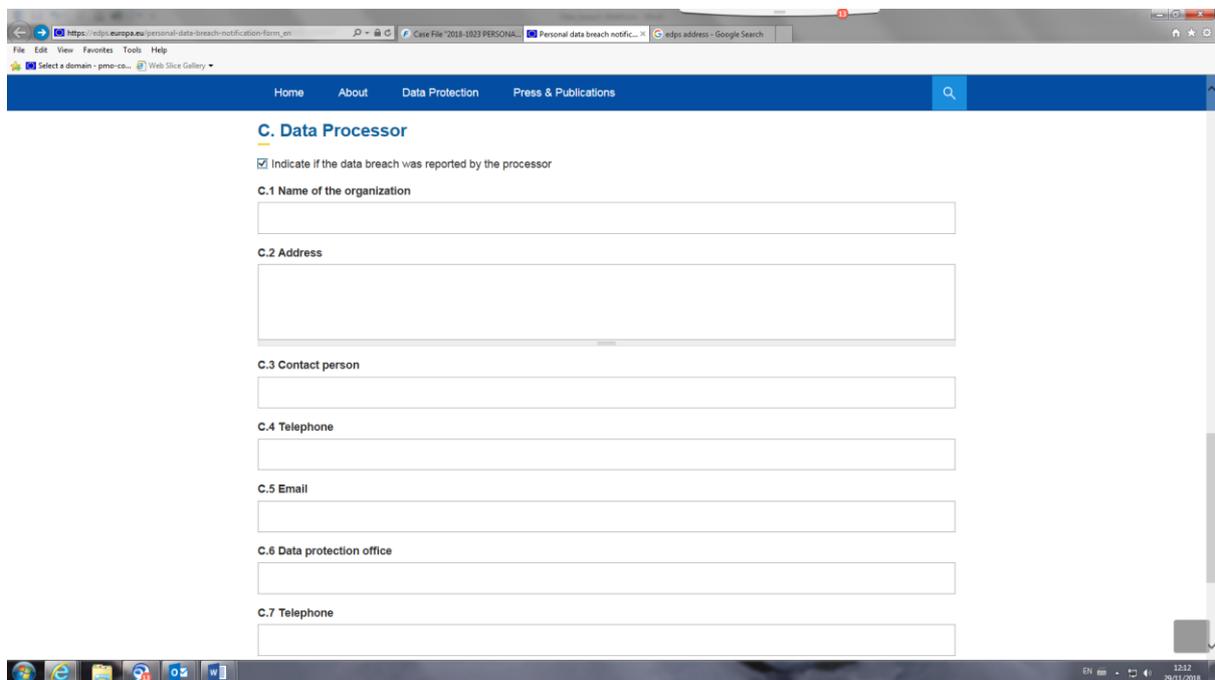
A screenshot of a web browser displaying the 'Personal data breach notification form' on the EDPS website. The browser's address bar shows the URL 'https://edps.europa.eu/personal-data-breach-notification-form_en'. The page has a blue header with navigation links: 'Home', 'About', 'Data Protection', and 'Press & Publications'. The main content area is titled 'C. Data Processor' and includes a checked checkbox for 'Indicate if the data breach was reported by the processor'. Below this, there are seven empty text input fields labeled 'C.1 Name of the organization', 'C.2 Address', 'C.3 Contact person', 'C.4 Telephone', 'C.5 Email', 'C.6 Data protection office', and 'C.7 Telephone'. The Windows taskbar is visible at the bottom of the browser window.

Abb. 4: Auftragsverarbeiter

Klicken Sie am Ende dieser Seite auf WEITER, um zum zweiten Abschnitt der Meldung zu gelangen.

ABSCHNITT II: Angaben zur Datenschutzverletzung

In diesem Abschnitt geben Sie alle wesentlichen Informationen im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten gemäß den Artikeln 34 und 35 der Verordnung an. Die Felder in diesem Abschnitt sind nicht obligatorisch und Sie können diesen Teil der Meldung mit den Ihnen vorliegenden Informationen ergänzen.

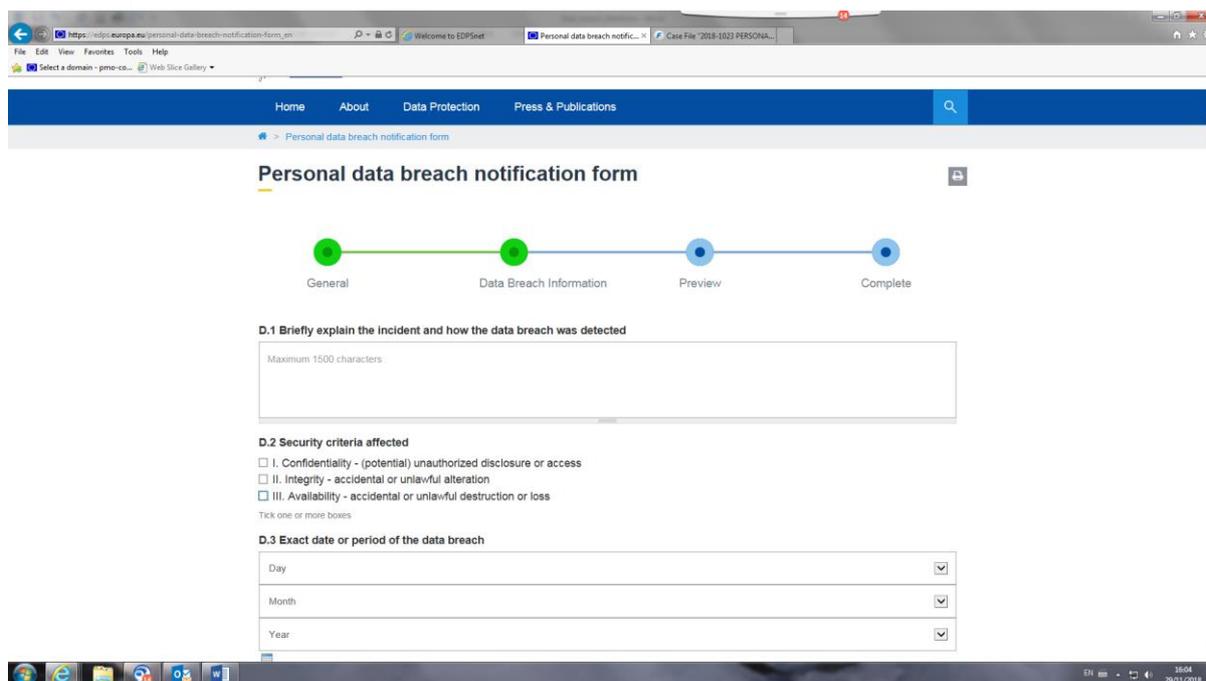


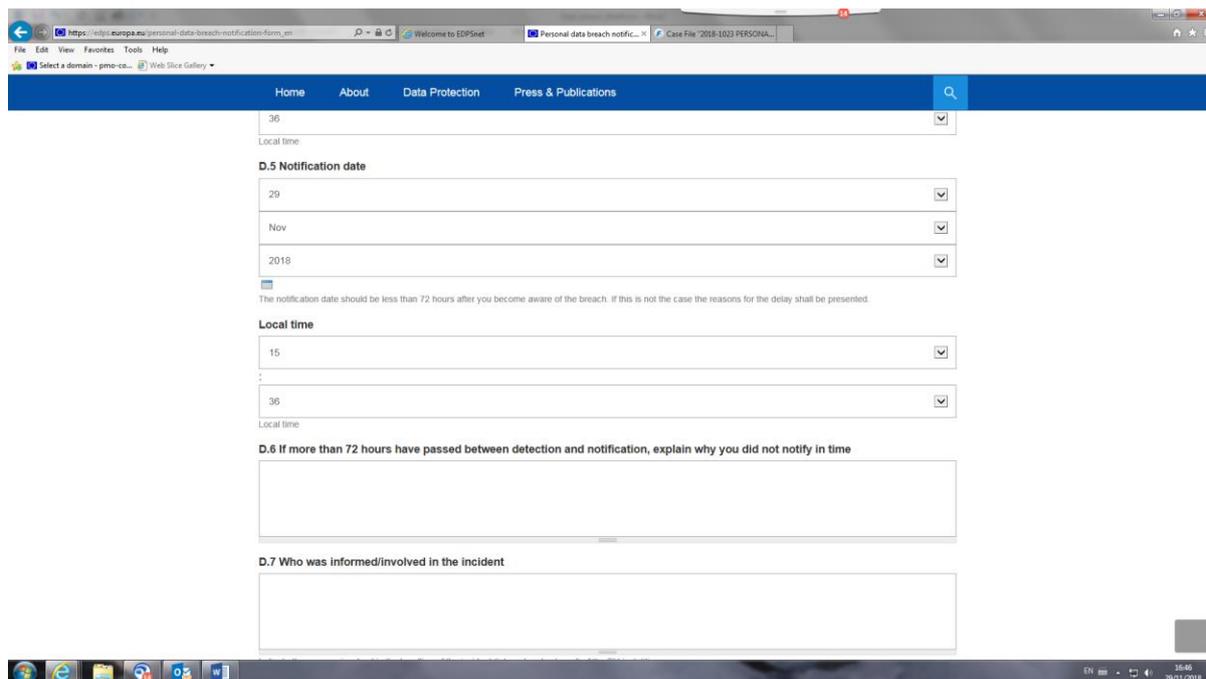
Abb. 5: Abschnitt II – Angaben zur Datenschutzverletzung (1)

D.1 Erläutern Sie kurz den Vorfall, und geben Sie an, wie die Datenschutzverletzung festgestellt wurde: Bitte beschreiben Sie in diesem Freitextfeld in kurzen Worten (höchstens 1 500 Zeichen) die Art der Datenschutzverletzung, deren Merkmale und Auswirkungen sowie die Art und Weise, in der dieser Vorfall festgestellt wurde.

D.2 Betroffene Sicherheitskriterien: Wählen Sie eine oder mehrere der drei Arten von Sicherheitskriterien aus, die von der konkreten Verletzung des Schutzes personenbezogener Daten betroffen sind, wobei Folgendes gilt: a) I. **Vertraulichkeit** – in Bezug auf die unbefugte Weitergabe oder den unbefugten Zugang zu personenbezogenen Daten; b) II. **Integrität** – in Bezug auf die unbeabsichtigte oder unrechtmäßige Änderung personenbezogener Daten; c) III. **Verfügbarkeit** – bei einer offensichtlich erkennbaren unbeabsichtigten oder unrechtmäßigen Vernichtung oder dem Verlust personenbezogener Daten.

D.3 Genaues Datum oder Zeitraum der Datenschutzverletzung: Bitte geben Sie hier durch Auswahl der entsprechenden Werte das genaue Datum der Datenschutzverletzung an; falls Ihnen das genaue Datum nicht bekannt ist, geben Sie im nächsten Feld den Zeitraum, in dem die Verletzung des Schutzes personenbezogener Daten aufgetreten ist, sowie weitere Informationen an.

D.4 Feststellungsdatum: Bitte geben Sie durch Auswahl der entsprechenden Werte das genaue Datum und den genauen Zeitpunkt (Ortszeit) an, zu dem Sie Kenntnis von der Verletzung des Schutzes personenbezogener Daten erhalten haben.



The screenshot shows a web browser window displaying the EDPS Personal Data Breach Notification Form. The browser address bar shows the URL: https://edps.europa.eu/personal-data-breach-notification-form_en. The page has a blue header with navigation links: Home, About, Data Protection, and Press & Publications. The form content includes:

- A dropdown menu for 'Local time' with the value '36' selected.
- A section titled 'D.5 Notification date' with three dropdown menus: '29', 'Nov', and '2018'.
- A note: 'The notification date should be less than 72 hours after you become aware of the breach. If this is not the case the reasons for the delay shall be presented.'
- A section titled 'Local time' with two dropdown menus: '15' and '36'.
- A section titled 'D.6 If more than 72 hours have passed between detection and notification, explain why you did not notify in time' with a large text input area.
- A section titled 'D.7 Who was informed/involved in the incident' with a large text input area.

Abb. 6: Angaben zur Datenschutzverletzung (2)

D.5 Datum der Meldung: Dieses Feld wird automatisch ausgefüllt. Überprüfen Sie das angegebene Datum und die Uhrzeit, und stellen Sie sicher, dass die Angaben in Bezug auf Ihre Meldung korrekt sind. Sofern nötig, nehmen Sie die erforderlichen Korrekturen vor.

D.6 Wenn zwischen der Feststellung und der Meldung mehr als 72 Stunden vergangen sind, erläutern Sie bitte, warum Sie den Vorfall nicht unverzüglich gemeldet haben: Bitte füllen Sie dieses Feld aus, wenn Ihre Meldung mehr als 72 Stunden nach Feststellung des Vorfalls erfolgt.

D.7 Wer wurde über den Vorfall informiert oder war daran beteiligt? Bitte geben Sie hier die Personen an, die an der Abwicklung dieses Vorfalls des EU-Organs beteiligt sind oder waren (intern und extern). Machen Sie umfassende Angaben.

D.8 Betroffene Kategorien personenbezogener Daten: Bitte führen Sie alle Elemente/Felder auf, die von der Datenschutzverletzung betroffene Daten enthalten, wie Vor- und Nachnamen, Geburtsdatum, Finanzdaten, Gesundheitsdaten usw., und erläutern Sie Ihre Auswahl.

D.9 Ungefähre Zahl der betroffenen personenbezogenen Daten: Bitte wählen Sie den korrekten Wert aus, und geben Sie, wenn möglich, die genaue Zahl der von der Datenschutzverletzung betroffenen personenbezogenen Daten an.

D.10 Betroffene Personenkategorien: Geben Sie die Kategorien der Personen an, die von der Datenschutzverletzung betroffen sind, z. B. EU-Bedienstete, MdEP, EU-Bürger, Kinder, benachteiligte Gruppen wie Menschen mit Behinderungen usw.

D.11 Ungefähre Anzahl der betroffenen Personen: Geben Sie, wenn möglich, eine genaue Anzahl für jede betroffene Personengruppe an, z. B. 150 MdEP, 2 000 europäische Bürger, 10 Kinder usw.

D.12 Wahrscheinliche oder tatsächliche Folgen der Datenschutzverletzung für die betroffenen Personen: Geben Sie, sofern bereits bekannt, die tatsächlichen oder

wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten für die betroffenen Personen an. Die Datenschutzverletzung kann körperliche, materielle oder immaterielle Schäden für die betroffenen Personen nach sich ziehen.

D.13 Abschätzung des Risikos für die Rechte und Freiheiten natürlicher Personen: Wählen Sie bitte das Ausmaß des Risikos: **Kein Risiko, Risiko, Hohes Risiko**

D.14 Erläutern Sie kurz, wie die Bewertung des Risikos für die Rechte und Freiheiten natürlicher Personen vorgenommen wurde: Bitte geben Sie an, wie Sie die Höhe des Risikos durch die Verletzung des Schutzes personenbezogener Daten festgestellt haben und ob Sie dazu eine bestimmte Methode verwendet haben.

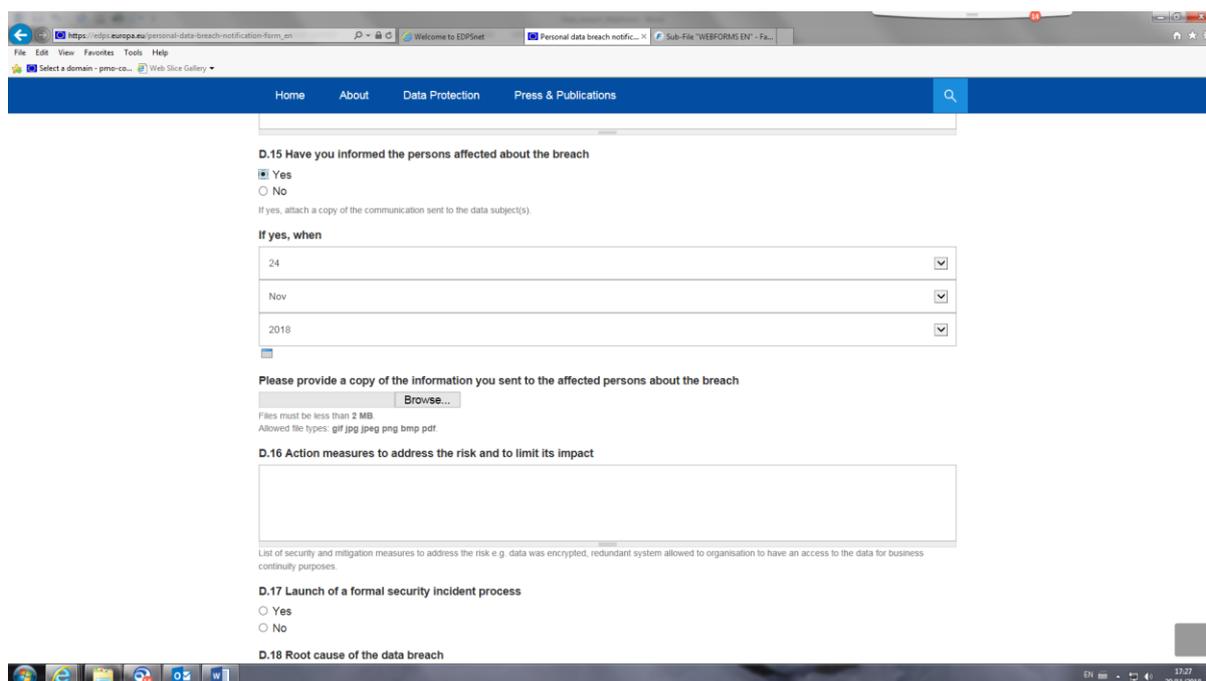
A screenshot of a web browser displaying the EDPS personal data breach notification form. The browser's address bar shows 'https://edps.europa.eu/personal-data-breach-notification-form_en'. The page has a blue header with navigation links: Home, About, Data Protection, and Press & Publications. The main content area contains several sections: 'D.15 Have you informed the persons affected about the breach' with radio buttons for 'Yes' (selected) and 'No', and a text area for 'If yes, when' containing dates '24', 'Nov', and '2018'. Below this is a 'Browse...' button for uploading a file, with a note that files must be less than 2 MB and lists allowed file types: gif, jpg, jpeg, png, bmp, pdf. The next section is 'D.16 Action measures to address the risk and to limit its impact' with a large text area. Below that is 'D.17 Launch of a formal security incident process' with radio buttons for 'Yes' and 'No'. The final visible section is 'D.18 Root cause of the data breach'. The Windows taskbar at the bottom shows the date and time as 17:27 on 29/11/2018.

Abb. 7: Inkenntnissetzung der natürlichen Personen

D.15 Haben Sie die betroffenen Personen über die Datenschutzverletzung informiert? Wählen Sie **Ja**, wenn Sie die betreffenden Personen bereits informiert haben, und geben Sie das Datum der Inkenntnissetzung an; **hängen Sie außerdem die Datei an**, aus der die Benachrichtigung der betroffenen Personen hervorgeht.

Wählen Sie **Nein**, wenn Sie die betroffenen Personen nicht informiert haben, und begründen Sie im Textfeld, warum Sie dies noch nicht getan haben.

D.16 Maßnahmen zur Eindämmung des Risikos und zur Begrenzung der Auswirkungen: Erläutern Sie kurz, ob Sie Sicherheits- und Abhilfemaßnahmen zur Eindämmung des Risikos ergriffen haben, z. B. eine Verschlüsselung der Daten oder redundante Systeme, die den Organisationen zur Aufrechterhaltung des Geschäftsbetriebs den Zugriff auf die Daten ermöglichen.

D.17 Einleitung eines formalen Sicherheitsvorfallverfahrens: Wählen Sie **Ja**, wenn ein formales Sicherheitsvorfallverfahren eingeleitet wurde. Wählen Sie **Nein**, wenn kein solches Verfahren eingeleitet wurde, und erläutern Sie die Gründe hierfür.

D.18 Ursache der Datenschutzverletzung: Erläutern Sie die Ursache des sicherheitsrelevanten Ereignisses, das zu dieser Datenschutzverletzung geführt hat.

Wenn Sie beide Abschnitte ausgefüllt haben, können Sie entweder auf ZURÜCK klicken, um zur vorherigen Seite zurückzukehren, oder auf **VORSCHAU**, um die von Ihnen angegebenen Informationen zu überprüfen.

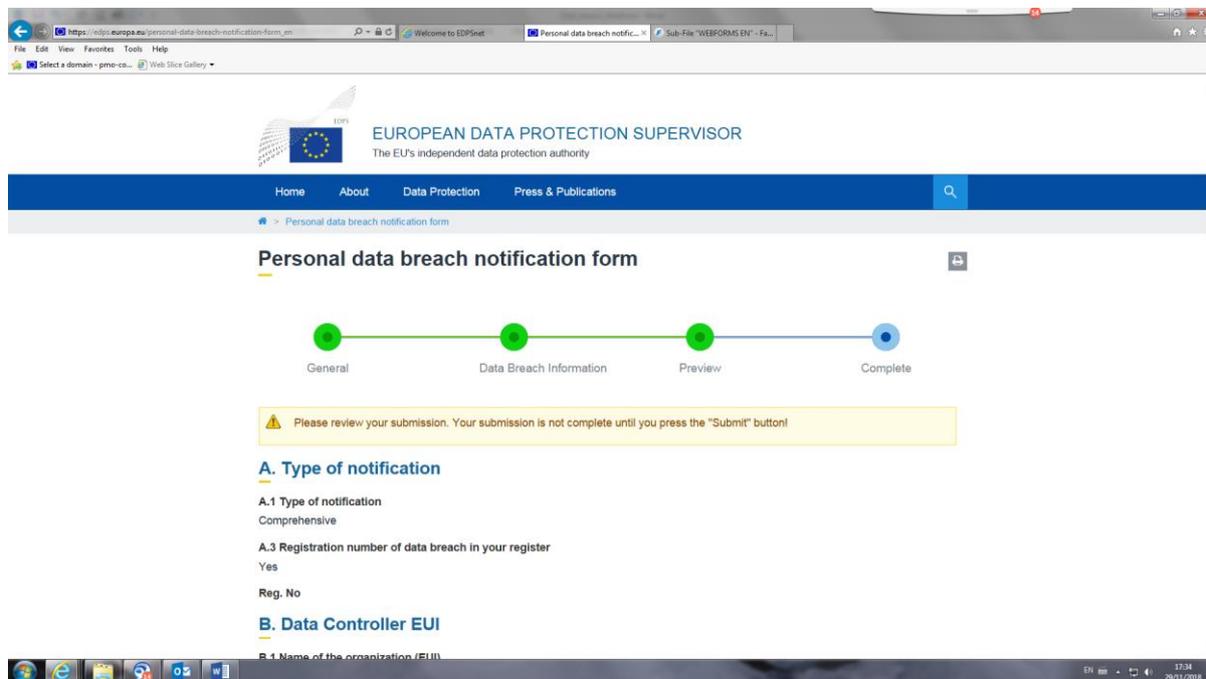
The screenshot shows a web browser window displaying the 'Personal data breach notification form' on the EDPS website. The page has a blue header with the EDPS logo and navigation links. A progress bar at the top indicates four steps: 'General', 'Data Breach Information', 'Preview', and 'Complete'. The 'Preview' step is currently active. A yellow warning box states: 'Please review your submission. Your submission is not complete until you press the "Submit" button!'. Below this, the form content is visible, including sections 'A. Type of notification' and 'B. Data Controller EUI'. The 'Type of notification' section shows 'Comprehensive' selected. The 'Data Controller EUI' section shows 'Name of the organization (EUI)' as the next step.

Abb. 8: Meldung der Datenschutzverletzung – Vorschau

Nachdem Sie sich eine Vorschau des ausgefüllten Formulars haben anzeigen lassen, klicken Sie bitte am Seitenende auf **ÜBERMITTELN**, um das Formular an den EDSB zu senden.

Sie erhalten folgende Nachricht:

NACHRICHT:

Vielen Dank, dass Sie eine Datenschutzverletzung gemeldet haben.

Sie erhalten innerhalb der nächsten Tage per E-Mail eine Eingangsbestätigung mit einer Fallnummer (Aktenzeichen), die Sie bei jeder künftigen Kommunikation mit dem EDSB angeben müssen.

Wenn Sie keine E-Mail erhalten, wenden Sie sich bitte an data-breach-notification@edps.europa.eu.

Im Anschluss an die oben genannten Schritte sendet der EDSB Ihnen innerhalb weniger Tage eine Bestätigungsmeldung mit einer spezifischen Fallnummer, die in allen künftigen Mitteilungen anzugeben ist.