EUROPEAN DATA PROTECTION SUPERVISOR

Data breach Web Form

User Guide

December 2018

TABLE OF CONTENTS

1 Introduction

The EDPS already provided the EU Institutions with the "*Guidelines on personal data breach notification for the European institutions and bodies*" where specific guidelines are provided regarding the notification obligation of article 34 of the Regulation 2018/1725 (EU).

The EDPS provides the controllers with two options:

1. Fill out the online form[1] in the EDPS Website : https://edps.europa.eu/form/personal-data-breach-notificatio_en
2. In case the first option is not possible to download a specific form and send it **encrypted**[2] directly to the functional mailbox: data-breach-notification@edps.europa.eu

2 Purpose

The purpose of this document is to provide instructions to the controllers on how to fill in the WebFom of Personal Data Breach, which is located in the EDPS Website.

3 WebForm Guidelines

The form Data Breach notification form is divided in two sections:

SECTION A : General

a) The section where you insert general information concerning the type of notification, the identification data of the controller and of the processor (if this applies to your case)

[1] Currently only available in English- EN. It will soon be available in French-FR and German -DE.

[2] When sending the form and any other attachment by email to the functional mailbox data-breach-notification@edps.europa.eu it shall be encrypted (zip), and the password shared with the EDPS by alternate means (by SMS or call). The EU institution will have to provide a separate telephone number in the email where the EDPS can contact for the password

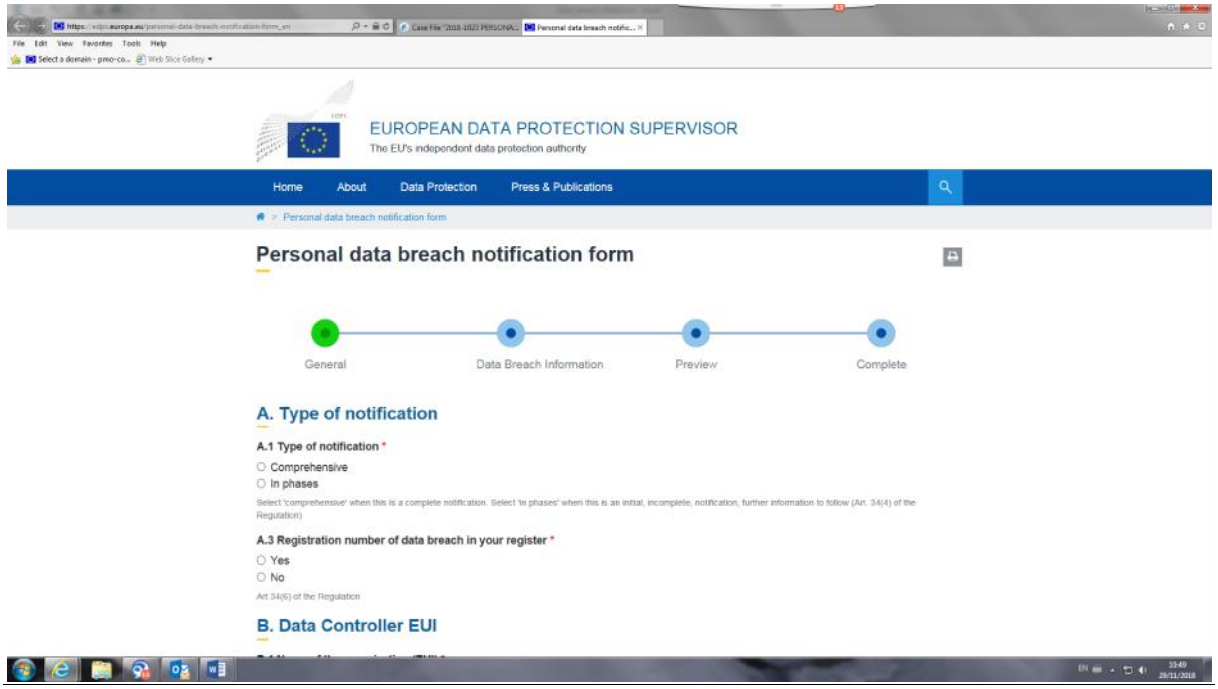

Figure 1 Personal Data Breach Form - General

A. Type of notification

In this section you shall choose the type of the personal data breach notification, either:

'Comprehensive' when this is a complete notification and you have all the information available concerning the personal data breach incident, or

'In phases' (Art. 34(4) of the Regulation2018/1725), when you don't have all the information available for the personal data breach incident because for example is still under investigation and you will submit the information in the future in more than one submissions.

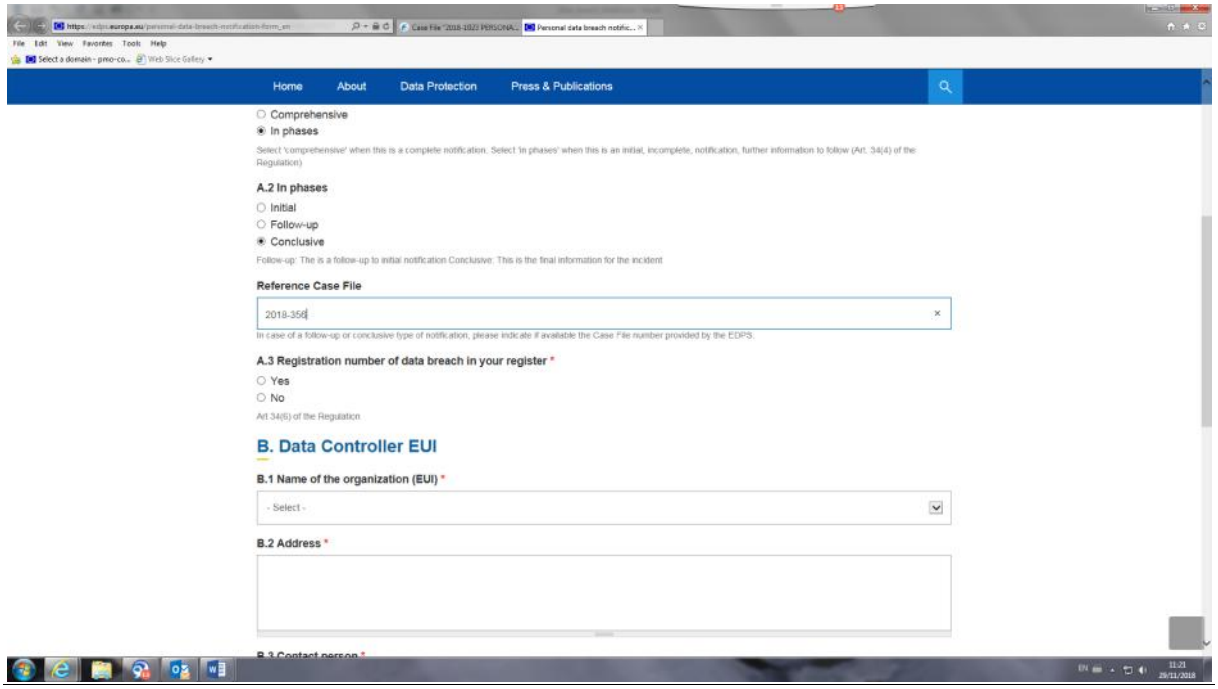

Figure 2 Notification In phases

A.2 In phases

In case you have chosen a notification "**In phases"** an additional selection appears and you have to specify if the notification is :

a) The first one where you have to choose "**Initial"**,

b) Is not the first one but also not the last one, where you have to choose "**Follow-up"** and

c) Is the final notification and you have to select **"Conclusive"**

For options b) and c) of above you will be requested to fill also the **Reference Case File** if you have it available from your initial submission. This is the number which EDPS has provided you by email and has the following format *YYYY-number*, e.g. 2018-356

A.3 Registration number of data breach in your register:

According to Art 34(6) of the Regulation 2018/1725, you shall document any personal data breach, comprising the facts relating to it, its effects and the remedial action taken.

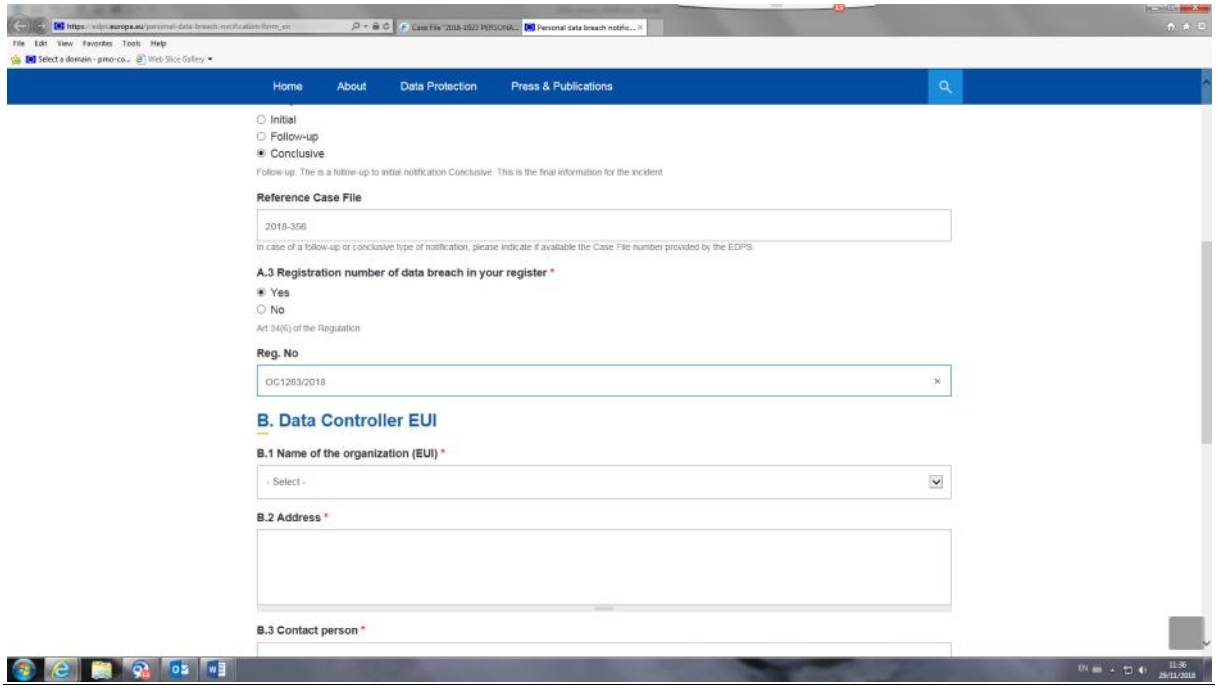

Figure 3 A.3 Registration Number

In case you have a specific registry (internal registry of the controller) established for this purpose please, select **Yes** and provide the specific reference if available *(e.g. number etc)* of the incident in your registry.

B. Data Controller EUI

In this section all the fields with (*) are mandatory and need to be filled in.

B.1 Name of the organization (EUI) : Please select the Name of your organisation from the drop-down list or select **Other** if not in the list and complete manually the name of your organization in the field **Please specify:** .

B.2 Address: Please complete the full address of your organisation, including Street name, number, Postal Code, Town/City and Country.

B.3 Contact person, B.4 Telephone, B.5 Email : Fill in the name, the telephone and the Email of the contact person for future communications with the EDPS on the specific case . Please take note that this email will be used by the EDPS when sending you the acknowledgement email in the end of your submission.

B.6 Data Protection Officer, B.7 Telephone, B.8 Email: Fill in the name, the telephone and the Email of the Data Protection Officer of your organisation.

C. Data Processor EUI

This section is optional and needs to be filled in only in cases where a personal data breach occurred in your data processor's processing activities (article 34(2) of the Regulation 2018/1725) and it was reported also by the processor.

In case this applies to you please *tick the box*: "**Indicate if the data breach was reported by the processor"**

The following fields will be activated and have to be filled in:

C.1 Name of the organization: Please fill in manually the Name of the processor organisation

C.2 Address: Please complete the full address of the processor, including Street name, number, Postal Code, Town/City and Country.

C.3 Contact person, C.4 Telephone, C.5 Email : Fill in the name, the telephone and the Email of the contact person of your processor for future communications with the EDPS on the specific case

C.6 Data Protection Officer, C.7 Telephone, C.8 Email: Fill in the name, the telephone and the Email of the Data Protection Officer of the processor.

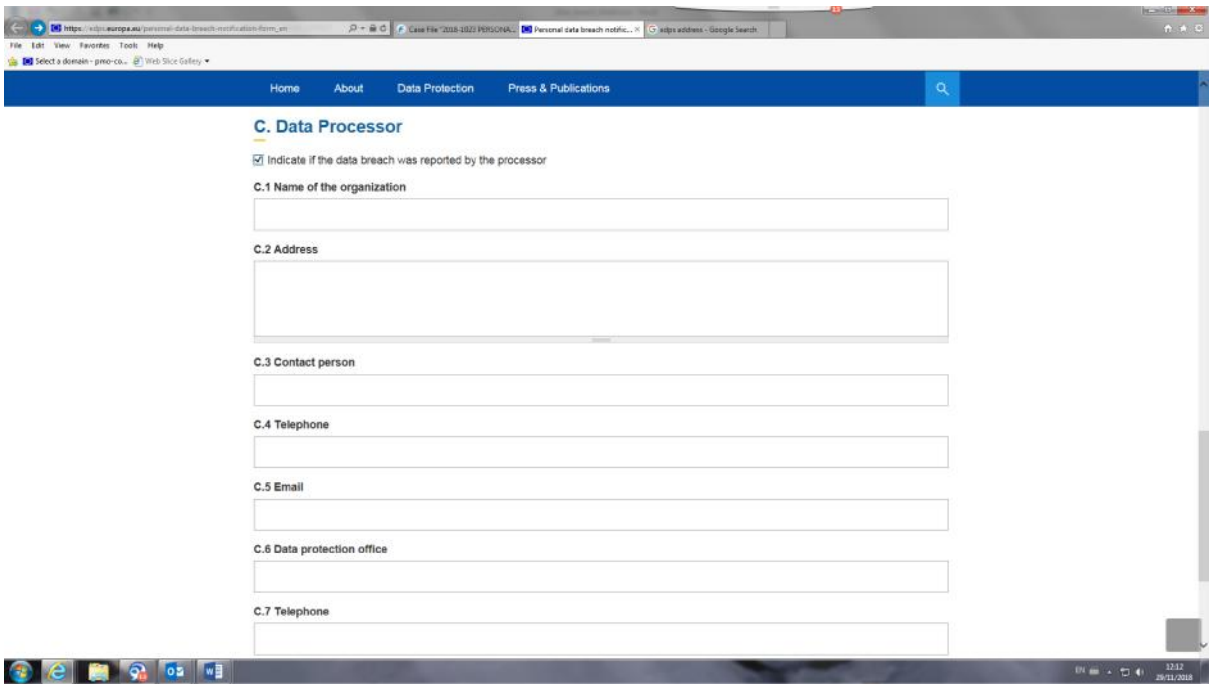

Figure 4 Data Processor

In the end of the page please press NEXT to move to the second section of the notification.

SECTION II: Data Breach Information

In this section you will provide the main details concerning the personal data breach incident as required by the articles 34 & 35 of the Regulation. All the fields of this section are not mandatory and you can fill this part of the notification with the information that you have available.

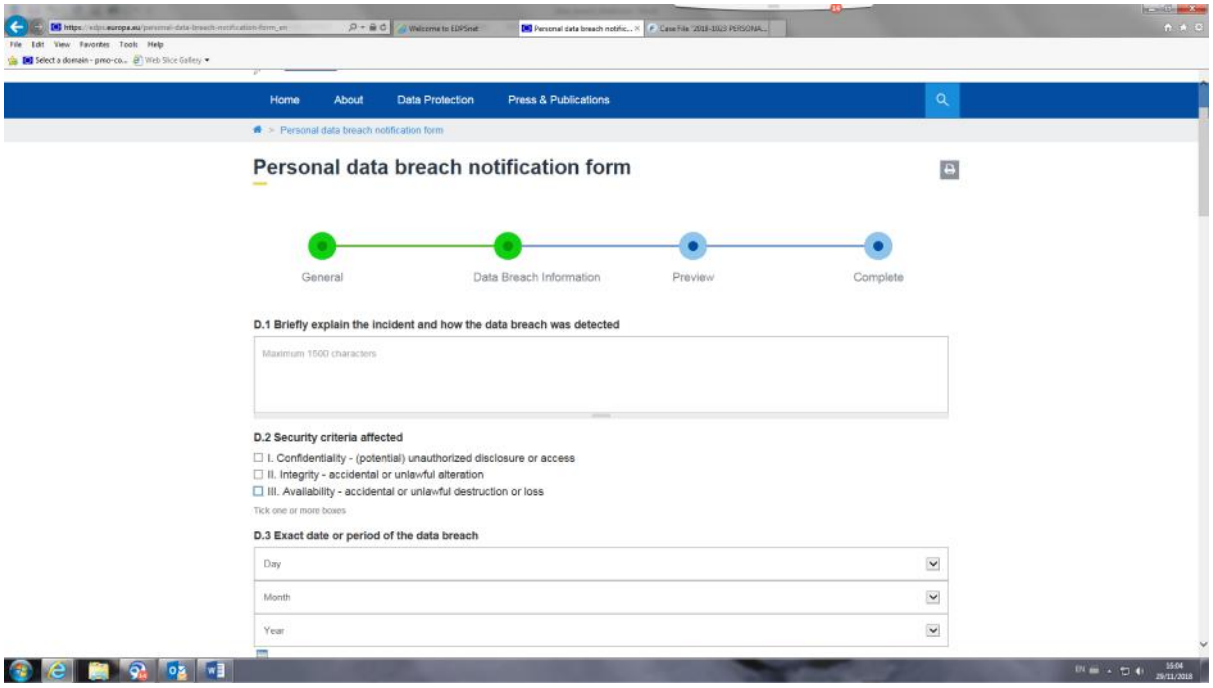

Figure 5 Section II : Data Breach Information(1)

D.1 Briefly explain the incident and how the data breach was detected: Please describe in the free text box (maximum 1500 characters) the nature, characteristics, effects of the personal data breach incident and how it as detected.

D.2 Security criteria affected: Select **one or more** of the three types of security criteria that were affected by the personal data breach incident, whereas a) I. **Confidentiality** - when it relates with unauthorized disclosure or access to personal information b) II. **Integrity** - when it relates with accidental or unlawful alteration of personal information and c) III. **Availability** - when accidental or unlawful destruction or loss of personal information was evident.

D.3 Exact date or period of the data breach: Please insert the exact date by selecting the correct values of the personal data breach, or, in case you are not aware of the exact date use the next field to insert the period of the personal data breach or other information.

D.4 Detection date: Please insert the exact date and the exact time (indicate your local time) when you became aware of the personal data breach by selecting the correct values in the boxes

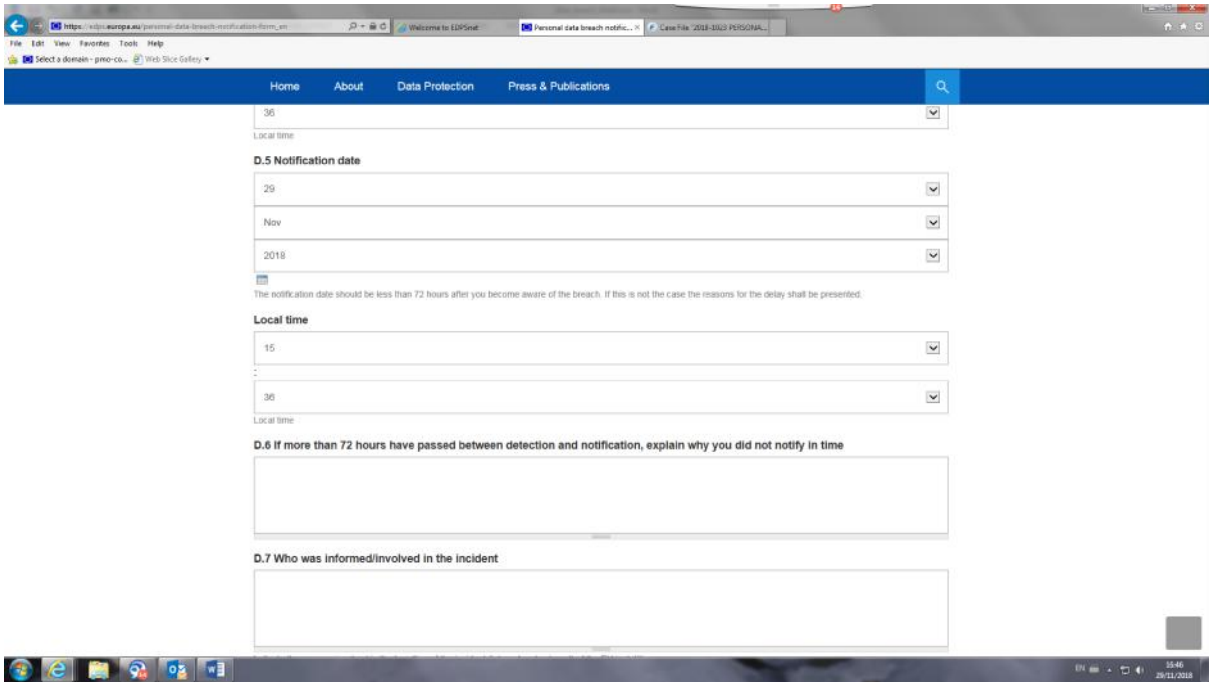

Figure 6 Data Breach Information (2)

D.5 Notification date: Please check and ensure that the indicative automatically filled current date and current time of the form is the correct one (indicate your local time) concerning your notification. If not make the necessary corrections.

D.6 If more than 72 hours have passed between detection and notification, explain why you did not notify in time: Please explain in case your notification is more than 72 hours late.

D.7 Who was informed/involved in the incident: Please indicate the persons who are or were involved in the handling of the incident (internal and external) of the EU institution. Provide comprehensive information.

D.8 Categories of personal data affected: Please explain and list all elements/fields of data that were compromised e.g. first and last names, date of birth, financial data, health data, etc.

D.9 Approximate number of personal data affected: Please select the correct value and if possible specify the exact number of the personal data that have been affected by the breach.

D.10 Category of persons affected: Provide the categories of the persons who are affected by the breach, e.g. EU staff, MEPs, European citizens, children, vulnerable groups such as handicapped people etc.

D.11 Approximate number of Persons affected: If possible provide a number for each category of persons affected, e.g. 150 MEPs, 2000 european citizens , 10 children etc

D.12 Likely or actual consequences of the data breach for the data subjects: Describe if you already know the actual or the likely consequences of the personal data breach to the data subjects. The data breach can result in physical, material or non-material damage to data subjects.

D.13 Estimation of the risk to the rights and freedoms of natural persons: Please select the size of the risk either: **None, Risk, High Risk**

D.14 Briefly explain how the assessment of the risk to the rights and freedoms of natural persons was done: Provide information on how you have assessed the level of risk of the personal data breach and if you have used a specific methodology.

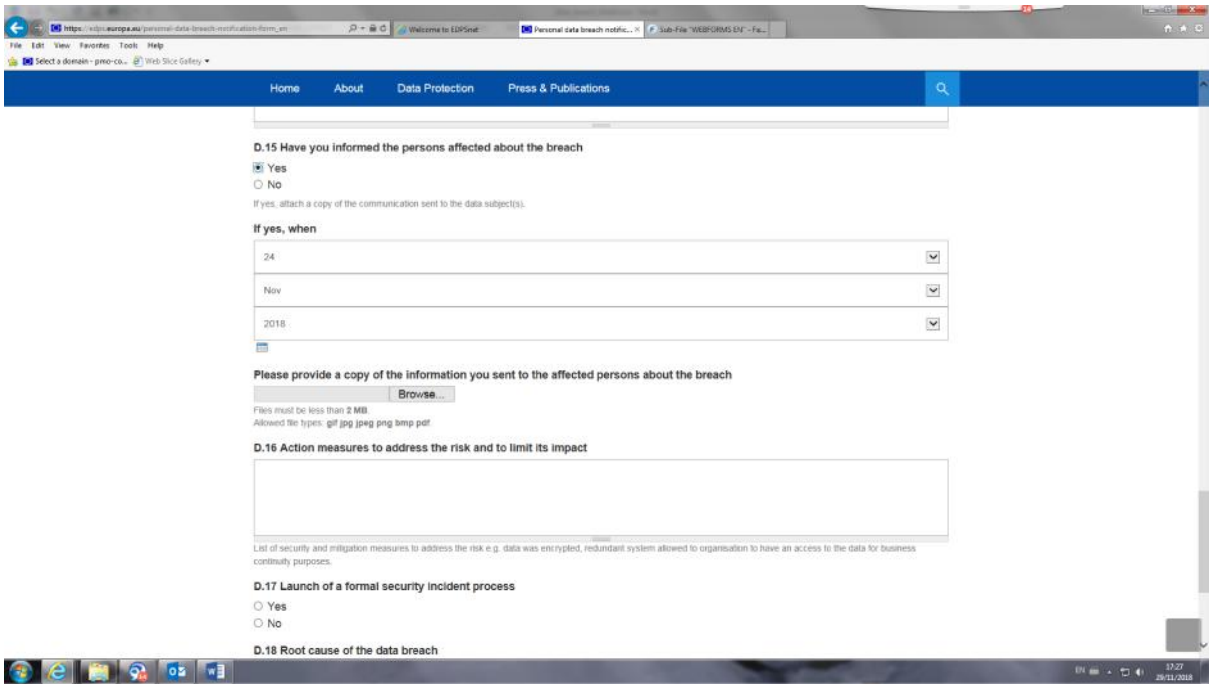

Figure 7 Information to the Natural Persons

D.15 Have you informed the persons affected about the breach : Please select **Yes** if you have already informed the persons and add the date you have sent that information and also **attach the file** containing the notification to the data subjects

Select **No** in case you have not informed the data subjects and provide more information in the text box why you have not done it yet.

D.16 Action measures to address the risk and to limit its impact : Briefly explain whether you have taken security and mitigation measures to address the risk e.g. data was encrypted, redundant system allowed to organisation to have an access to the data for business continuity purposes.

D.17 Launch of a formal security incident process Please select **Yes** if a formal security incident process has been launched. Select **No** if no such process has been initiated and explain the reasons.

D.18 Root cause of the data breach: Explain the root cause of the security incident that lead to the data breach.

After the completion of the two sections, you can either press PREVIOUS and move to the previous screen or press PREVIEW to review the information you have provided.

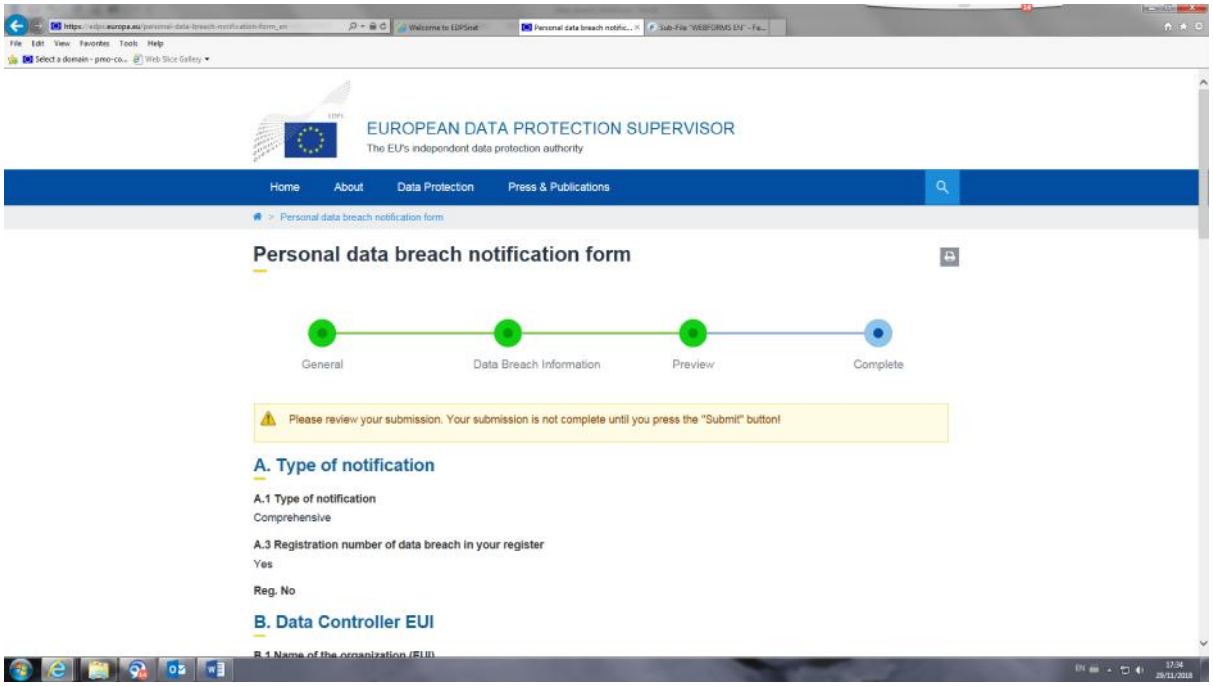

Figure 8 Preview of the DBN

After you have previewed the form please press **SUBMIT** at the bottom of the page to submit the form to the EDPS.

You will receive the following message:

MESSAGE

Thank you for your submission of a Data Breach Notification.

You will receive a manual acknowledgement email within the next days with a Case Reference Number, which you will use for future communications with the EDPS.

If you get no email, please contact us at data-breach-notification@edps.europa.eu

Following the above EDPS will send you within a couple of days a confirmation message indicating a specific Case Reference Number for your notification that will be used in future communications.