



GDPRiS Platform v2 Guidance for Users

Document Version: 1.0
Revision Date: 09/03/2022

General Staff

Incident Log

Important Notice:

© GDPR in Schools Ltd 2021. All rights reserved.

This document and the associated software are the sole property of GDPRiS. Reproduction or duplication by any means of any portion of this document without the prior written consent of GDPRiS is expressly forbidden.

GDPRiS reserves the right to make changes to this document and to the related software at any time without notice. The information in this document has been carefully checked for its accuracy; however, GDPRiS makes no warranty relating to the correctness of this document.

Incidents

The aim of the Incident Log is to provide you with a central location to log both Data Breaches and Cyber-attacks.

Historically the GDPRiS portal only allowed users to log data breaches, now the portal can cater for both data breaches and cyber-attacks. Since both data breaches and cyber-attacks are classed as Incidents, we have introduced a new section called “**Incident Log**”.

Incident typical meaning – “an action likely to lead to grave consequences”

Add an Incident

Navigate to **Incident Log** via the tile on the **Dashboard** or **Incident Log** on the **Navigation Pane**.

Click the **Add Incident** button and a pop-up window will appear.

Fill in the relevant information required:

Discovered – When the Incident came to the attention of a member of staff

Title – A rough descriptive title which identifies what the incident refers to

Description – Describe what has happened with regards to the incident however please refrain from adding any personal identifiable information.

Type – You can select either a Breach or a Cyber Incident or both depending on the type of Incident which you are raising. If you are unsure, you can leave as unselected.

Attach Document – An option has been provided for you to attach a document if required.

NB. Once added this cannot be deleted.

The image shows two side-by-side screenshots. The left screenshot is a form titled "Add Incident". It has a dropdown menu for "Discovered" with "Discovered" selected. Below it is a "Title" text input field, followed by a larger "Description" text area. At the bottom, there are two checkboxes: "Type (optional)" with "Breach" and "Cyber Incident". Below the checkboxes are two buttons: "+ Choose" and "X Cancel". At the very bottom is a dashed box for file upload with the text "Drag and drop files here to upload" and an "+ Add" button. A red arrow points from the "Discovered" dropdown to the right screenshot. The right screenshot is a calendar widget for April 2021. The date "1" is selected and highlighted with a blue border. The calendar shows days of the week (Su, Mo, Tu, We, Th, Fr, Sa) and dates from 28 to 1. Below the calendar are navigation arrows and a time display "12 : 53". At the bottom are "Today" and "Done" buttons.

Facts Card

Once the Incident has been created you will be shown the “**Facts Card**” for you to fill in, to the best of your abilities to provide as much information as you can regarding the Incident.

The purpose of the Facts Card is to provide as much information as you can as the raiser of the incident so that the appropriate members of staff can use that information in dealing with the incident.

Fill in as much information as you can and then click “**Save**” if you have made changes or “**Close**” if you simply wish to skip this page at this moment in time. You will be able to come back to the **Facts Card** later in the process if you choose to.

←

Facts Card

In order to help investigate this incident thoroughly, please write down all you know about the incident. The Text boxes will prompt you into supplying the information that will help. Please give as much factual information as you can. Feel free to skip questions that you don't know the answers to. Every bit of information will contribute to the response effort. Please avoid putting unnecessary personal information into your answers, especially when it relates to non-staff.

<p>Date of Incident</p> <input style="width: 95%; height: 20px;" type="text"/>	<p>Who's data has been involved? How many individuals' data are involved?</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>Reported By</p> <div style="display: flex; align-items: center;"> <input style="width: 80%; height: 20px;" type="text"/> <div style="margin-left: 5px;"> Alternative reported by name </div> </div>	<p>If there are any systems compromised, who has or had access to these systems?</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>How was it detected?</p> <input style="width: 95%; height: 20px;" type="text"/>	<p>Who has received/stolen/accessed the data?</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>What makes you think this is or isn't a cyber security incident? How many data records and data subjects are affected?</p> <input style="width: 95%; height: 20px;" type="text"/>	<p>If applicable: Where was the data lost?</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>What makes you think this is or isn't a data incident? How many data records and data subjects are affected?</p> <input style="width: 95%; height: 20px;" type="text"/>	<p>Have you taken any actions so far?</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>What locations are involved?</p> <input style="width: 95%; height: 20px;" type="text"/>	<p>Was this intentional or caused by negligence (e.g. human error through a phishing campaign)?</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>Which members of staff are involved?</p> <input style="width: 95%; height: 20px;" type="text"/> <p style="font-size: 0.7em; margin-top: 5px;">xxx 3/5000 char(s)</p>	<p>What technical data has been captured? (IP addresses, machine names, user names)</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>Who is aware of the event?</p> <input style="width: 95%; height: 20px;" type="text"/>	<p>Was a vulnerability exploited? Who might have known about the vulnerability?</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>What data, systems, applications, documents etc. are involved?</p> <input style="width: 95%; height: 20px;" type="text"/>	<p>Any other detail</p> <input style="width: 95%; height: 20px;" type="text"/>
<p>What categories of personal data are at risk or have been breached?</p> <input style="width: 95%; height: 20px;" type="text"/>	

✕ Close
💾 Save

Contact the Customer Success Team

Office hours

Mon-Thurs: 09:00 - 16:30 GMT

Fri: 09:00 – 15:30 GMT

If you require assistance regarding any section of this help guide, please do not hesitate to contact us via one of the following methods:

Tel: 02039 610 110

Mail: support@gdpris.co.uk