Data Protection Statement for the Fire & Flood DataBase

THE FIRE PROTECTION ASSOCIATION & RISCAUTHORITY

INTRODUCTION

This Data Protection Statement explains in detail the types of data we collect in the Fire & Flood DataBase. It also explains how we will store and use that data and keep it safe. The Fire & Flood DataBase was previously referred to as the Large Loss DataBase (or LLDB) but was renamed in 2021 to reflect an increase in its scope to incorporate significant flood related losses.

We hope the following sections will answer any questions you may have but if not, please do get in touch with us on 01608 812500 or email us at info@riscauthority.co.uk.

It is possible that we will need to update this Data Protection Statement from time to time. We will notify you of any significant changes, but you are welcome to come back and check it whenever you wish.

By using the Fire & Flood DataBase upload site, you are assumed to agree with this Data Protection Statement and give us permission to process the data you provide specifically for the purposes identified here.

1. WHO ARE THE FIRE PROTECTION ASSOCIATION & RISCAUTHORITY?

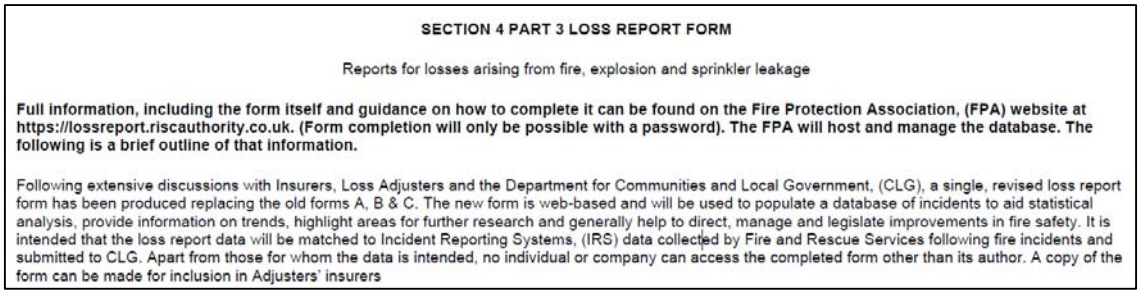
The Fire Protection Association (FPA) was established in 1946 by the Association of British Insurers (ABI) to be the core voice of fire safety for the Fire Offices' Committee. Our remit is to promulgate best practice guidance for the protection of life, property, business and the environment, from sundry insurance perils. The FPA is the UK's national fire safety organisation. We work to identify the dangers of fire and help our clients reduce any fire-related risks. As fire safety experts, we have an unrivalled reputation for quality and expertise in all aspects of fire protection including research, consultancy, training, publications, risk surveying and auditing. All our services are central to the reputation we have built amongst our membership and advocates who trust our expertise. We actively seek to move fire safety standards forward by lobbying government and working with them to address our issues and concerns.

RISCAuthority (Risk, Insight, Strategy and Control Authority) conducts research and representation on behalf of a group of UK Insurers relating to risk mitigation measures from fire and other insured perils. The prime objectives of the scheme are:-

- to identify issues currently affecting the UK insurance industry and invest accordingly
- to maintain and improve current insurer fire protection practice
- to make fire and property protection financially and technically attractive to the insured property owner
- to act as a focal point for all stakeholders with interests in fire protection
- to encourage commonality with Government policy where prudent

2. WHAT IS THE FIRE & FLOOD DATABASE ?

The Fire & Flood DataBase (hereafter referred to as the 'F&FDB') is a repository of important information on significant fire and flood losses within the UK. RISCAuthority originally introduced this system many years ago to replace the paper-based methods formally administered by ABI as described in Section 4 of the 'Blue Book' – Claims Management:



SECTION 4 PART 3 LOSS REPORT FORM

Reports for losses arising from fire, explosion and sprinkler leakage

Full information, including the form itself and guidance on how to complete it can be found on the Fire Protection Association, (FPA) website at https://lossreport.riscauthority.co.uk. (Form completion will only be possible with a password). The FPA will host and manage the database. The following is a brief outline of that information.

Following extensive discussions with Insurers, Loss Adjusters and the Department for Communities and Local Government, (CLG), a single, revised loss report form has been produced replacing the old forms A, B & C. The new form is web-based and will be used to populate a database of incidents to aid statistical analysis, provide information on trends, highlight areas for further research and generally help to direct, manage and legislate improvements in fire safety. It is intended that the loss report data will be matched to Incident Reporting Systems, (IRS) data collected by Fire and Rescue Services following fire incidents and submitted to CLG. Apart from those for whom the data is intended, no individual or company can access the completed form other than its author. A copy of the form can be made for inclusion in Adjusters' insurers

Submissions to the database are made on insurers' behalf by the loss-adjusting community, usually as part of their contract, for incidents meeting one or more of the following criteria:

- material damage for all interested parties exceeding £100,000
- business interruption is estimated at over £100,000
- where the combined figure from material damage and business interruption is expected to exceed £100,000
- whenever there is a fatality, regardless of the above
- following any sprinkler actuation regardless of the above

3. WHY IS FIRE & FLOOD DATA IMPORTANT?

The contribution of loss data by the adjusting teams is essential to the work of RISCAuthority and the support it provides to the insurer membership. Analysis of the dataset enables interrogation of factors that contribute to loss incident prevalence, the extent of loss, and factors that acted beneficially or detrimentally to the outcome. The data is used by RISCAuthority for horizon-scanning purposes to identify research needs and is made available to insurers to support their own risk analysis and mitigation initiatives.

4. WHAT DATA DO WE COLLECT?

Personal Data

Personal data refers to any information which identifies a person, or which can be identified as relating to someone personally, such as their name, address, phone number and email address. No personal data is collected or stored with the F&FDB itself. However, RISCAuthority does collect some personal data provided by individuals when they register for a user account of the F&FDB and that particular data is covered by our privacy policy which can be found here: https://www.riscauthority.co.uk/about-us/privacy-policy

Sensitive and Non-Sensitive Data

Section 5 details how we use data that is collected and stored within the F&FDB, and in particular explains what aspects of the data is and is not shared with members of RISCAuthority. In summary, no data that has been identified as being Sensitive will ever be published by RISCAuthority or shared with any party other than the owner(s) of that data.

Any data field within the database that could potentially be used to identify the insured party, the insurer(s), the loss adjuster, or the incident itself, associated with a case record is considered Sensitive Data. Data fields that cannot obviously be used to identify an incident or any associated parties, and which is considered to be of useful and legitimate interest for analysis are considered to be Non-Sensitive Data which may be used (as detailed in section 5) in Aggregate data sets. All Sensitive Data fields will always be fully redacted in any Aggregated data sets.

The specific details of which data fields are identified as being Sensitive and Non-Sensitive has been agreed with the F&FDB working group (comprising representatives from each member company) and will be reviewed annually. A full list of the data fields used in the F&FDB, including details of what are considered Sensitive and Non-Sensitive Data, can be provided upon request (please contact cford@thefpa.co.uk). An overview of the types of data collected within the F&FDB is summarised below.

Free text fields are considered Sensitive Data due to a lack of control over their population by the loss adjuster.

Loss Adjuster Data

The company name and address of the loss adjuster associated with each case is collected and stored within the F&FDB. All loss adjuster data is classed as Sensitive Data.

Basic Case Data

The date and time of each incident is recorded, as is the name of the insured party and the Fire & Rescue Service IRS reference number. Each of these items is classed as Sensitive Data.

However, the incident date and time are special cases and are treated slightly differently to all other Sensitive Data with regards to how the information is presented in anonymised aggregate data sets. Whereas all other Sensitive Data is fully redacted and replaced with a sequence of hash's as "##########", the incident date and time are partially redacted as follows to allows for temporal analysis of events without revealing the exact date or time of any one incident:

- Incident dates are collected in the format dd/mm/yy. In anonymised aggregate data sets, a date is included, however the 'day' for every case is set to the first day of the month. For example, an incident occurring on 23/07/19 would appear in an aggregated data set as 01/07/19, as would a second incident that had occurred on the 18/07/19.
- Incident times are collected in the format hh:mm:ss. In anonymised aggregate data sets the 'time' of an event is only indicated as having occurred in one of four time periods:
  - 00:00 – 05:59
  - 06:00 – 11:59
  - 12:00 – 17:59
  - 18:00 – 23:59

  The actual recorded event time is fully redacted.

Financial Loss Data

A range of information relating to the financial loss aspect of each incident is collected and stored within the F&FDB. Information is collected on each of the following insurance elements;

- Business insurance
- Contents insurance
- Stock insurance
- Business interruption insurance
- Rent insurance
- Machinery and plant insurance
- Other insurance

For each of these elements several data points are recorded, including;

- The insurer company name
- The total sum insured (TSI)
- The estimated loss value
- The final loss value
- Any deductible amounts
- Any amounts not paid due to underinsurance
- Whether the insured element was repudiated
- Whether the insured element was withdrawn

With the exception of the insurer's name (which is considered Sensitive Data) all of the above information is classed as Non-Sensitive Data.

Insurance Policy Numbers

Policy numbers for each insurance type (Business, Contents, Stock, Business interruption, Rent, Machinery, and plant, Other) are collected and stored within the F&FDB. All policy numbers are (as are all case specific reference numbers) classed as Sensitive Data.

Business Type Data

Information is collected about the business sector in which the incident occurred and the specific type of business involved (e.g., Sector = Industrial Processing and Manufacturing; Business Type = Printing). This is classed as Non-Sensitive Data.

Incident Type Data

A range of information relating to the incident itself is collected and stored within the F&FDB including;

- Primary cause of the fire (e.g., accidental or deliberate)
- Cause of the fire (e.g., Cooking appliance – Deep fat frier)
- Location of the fire (e.g., Building – Kitchen)
- The type and scale of damage caused (e.g., smoke – 3 floors – 500m^2)
- The number of people that died or were injured
- Factors that affected any firefighting efforts (e.g., inadequate water supplies)

This is classed as Non-Sensitive Data.

Property Type Data

Certain information relating to the affected property is collected and stored within the F&FDB including;

- The building occupation (e.g., occupied or un-occupied)
- The building status (e.g., under construction, completed, or in refurbishment)
- The building situation (e.g., attached, semi-detached, or detached)
- Special features (e.g., is the property listed, or in a conservation area)

This is classed as Non-Sensitive Data.

Construction Type Data

A range of information relating to construction details of the affected property is collected and stored within the F&FDB including;

- The building's overall construction category (e.g., Cat2a Non-Combustible)
- Materials used in the buildings structure, roof, and cladding (e.g., brick and stone, light timber frame, steel & glass, etc)

This is classed as Non-Sensitive Data.

Detection and Suppression Type Data

Information relating to fire protection systems within the affected property is collected and stored within the F&FDB including;

- Was automatic fire detection installed? If so, was it linked to an alarm receiving centre and did it detect the fire?
- Was there a fixed fire suppression system installed? If so, what type was it (e.g., sprinklers, water mist, dry powder, etc) and did it control or extinguish the fire?

This is classed as Non-Sensitive Data.

Flood Data

Until 2020 the F&FDB exclusively recorded data on losses related to fire incidents. However, at the request of RISCAuthority members the F&FDB upload site was modified in 2020 to allow significant flood related incidents to also be recorded. Much of the data collected is the same as detailed in the preceding paragraphs, including:

- Loss Adjuster Data
- Financial Loss Data
- Business Type Data
- Property Type Data
- Construction Type Data

The level of sensitivity of this data is likely to be identical to that of the equivalent fire loss data records that is detailed above.

Additionally, a range of information is collected relating to the flood incident, the type and extent of damage caused, any flood protection measures in place, and details about recovering from the flood. All of which is likely to be classed as Non-Sensitive Data.

As of 2021 there are very few flood related entries in the F&FDB and consequently there is currently no intention to make any flood data available for analysis. At such time as it is considered appropriate to make this data available, the membership will be consulted as was done with the fire loss data to agree on what elements of the dataset should be classed as Sensitive and Non-Sensitive.

5. HOW WE USE LOSS DATA ENTERED INTO THE F&FDB

FPA and RISCAuthority are independent and not for profit organisations. The collection and provision of large loss case data is undertaken at the request of, and for the benefit of, the RISCAuthority member companies. FPA and RISCAuthority will never sell or otherwise share any identifiable or specific case data. However, FPA and RISCAuthority may publicise selected summarised aggregate data statistics for lobbying, training, or risk awareness purposes. A typical example would include publishing the numbers of cases and total/average case loss values for specific business types in the Business Sector Risk Review reports that are produced by RISCAuthority.

No data classed as Sensitive (see section 4) will ever be released or shared with anyone outside of the loss adjuster and the associated insurance company that submitted the data originally.

Aggregated data sets will be made available through the F&FDB download website to all, and only, RISCAuthority member companies.

Aggregated data sets will always be anonymised, with all data classed as Sensitive being redacted to remove any information that might allow specific cases to be identifiable. The specific details of what information may be shared and what should be redacted has been agreed with the F&FDB working group (comprising representatives from each member company) and will be reviewed annually.

The aggregated data sets made available through the F&FDB website may be used by RISCAuthority members for their own purpose, such as comparison with their own loss data. However, specific case information from these aggregate data sets may not be shared or published outside of each members' own company.

6. PROVIDING OUR SERVICES TO YOU AND RISCAUTHORITY MEMBERS

Products and services

RISCAuthority will host, maintain, and support the F&FDB upload website and the F&FDB download website until instructed to do otherwise by the membership.

We will use the data you provide us with in support of the aims of the RISCAuthority scheme as detailed in sections 1 and 5. We will provide tools to enable members to download and analyse both case data pertaining to their own company and anonymised aggregate data sets.

Marketing, Advertising, Profiling and targeting

We will never use any of the information entered into the F&FDB to contact you for the purposes of marketing, advertising, profiling, or targeting information.

Emailing

We will only contact loss adjusters should an issue arise relating to their user account, or case data that they have entered on the F&FDB, or in response to an enquiry that they have raised.

The F&FDB upload site does however include an automated email reminder system which will periodically contact loss adjusters if they have omitted to provide key case data.

Cookies and third-party websites

Cookies

Our websites use cookies to distinguish you from other users to help us provide you with a personalised experience and to improve our websites and services.

A cookie is a small text file that is placed on your computer's hard drive by your web browser when you first visit our website. The cookie allows us to identify your computer and find out details about your last visit to the website.

The information we collect by using cookies is not personally identifiable: it does not include information about your computer settings, your connection to the internet, IP address or geographical location.

Third-party websites

The RISCAuthority F&FDB data upload website links to the FPA website, which in turn provides links to external websites for your convenience. These external websites will have their own privacy policies, and if you click on a link our Data Protection Policy and Privacy Policy will no longer apply. We do not accept any responsibility or liability.

Protecting you and our business from crime

As detailed in RISCAuthority's privacy policy (https://www.riscauthority.co.uk/about-us/privacy-policy) we use your user account data to help protect our business and your account from fraud and other illegal activities, including using your data to maintain, update and safeguard your account.

We will also monitor your browsing activity with us to quickly identify and resolve any problems and protect the integrity of our websites. For example, using automated monitoring of unsuccessful login attempts to identify possible fraudulent attempts to gain access to your account.

7. HOW WE PROTECT YOUR DATA

We know how much data security matters to all our members and we want to keep your data and our information systems safe and secure. We treat your data with the utmost care and are committed to taking all appropriate steps to protect it.

All new staff complete mandatory data protection training when they start working for the FPA and this is repeated by all staff annually.

Although we take all reasonable steps to keep your information safe and secure, external threats are constantly evolving and we cannot guarantee the absolute security of your information.

Data Storage

The F&FDB upload application is hosted on a secure cloud (Microsoft Azure) within a UK datacentre, with backups stored in a different UK datacentre. Data stored using Azure SQL Server is encrypted at rest.

Access to the application source code and database is password controlled and limited to the RISCAuthority Administration team.

Data backups are stored on a secured filesystem.

Data Transport

The application implements Sitewide SSL with Strict Transport Security using industry standard SHA256RSA encryption via a verified certificate. The default protocol is TLS 1.2. Insecure cipher suites are disabled (i.e., legacy TLS 1.x, SSL2 & 3)

Backend data transfer between FPA back-office and the Azure cloud is similarly encrypted as above.

Application Security

Client Software

The application operates as Software-As-A-Service (SAAS), is accessible via web browser and requires no software to be installed on the client.

Server Software

The application is implemented in the C# language using the Microsoft MVC4/ASP.NET framework, LinqToSQL and SQL Server.

Cross Site Scripting Attacks

The user is prevented from injecting scripts via the user interface, such input is detected and rejected by the application. User input is mediated through typed parameters in LinqToSQL and SQL Server stored procedures.

Application output is html-encoded so that any scripts injected into the database cannot execute on the browser.

Use of Secure Cookies

The application requires “Secure Cookies” requiring the browser to limit transmission of cookie data to encrypted channels.

Individual User Accounts

Corporate and Individual accounts are secured with a username and password.

Application Data Visibility

Insurer corporate accounts are limited to viewing cases relevant to their company. In cases where multiple insurers cover a single case Insurers can only view financial information relevant to their company (an insurer can see that another company is involved but not the financial details of their interest).

Loss Adjuster corporate accounts have visibility of cases limited to their involvement.

Loss Adjuster individual accounts have visibility of cases limited to those which they created and to those in which their main company has an interest. Where two Loss Adjuster Companies have merged, Loss Adjusters also have access to the merged company cases.

Password Resets

A user can reset their password at any time. Password resets are transacted through the application (i.e., over SSL). Password resets can only be performed by obtaining a temporary token relayed to the registered email address of the user.

Personal information and GDPR

Users accounts are limited to storing the following personal information: corporate email, name, employer, and address. Accounts and their commensurate data are removed if inactive for a prescribed period.

Personal Information is not required to be input in the normal course of business; however, the application does not prevent this and so Personal Information may occur in correctly entered data. The application provides for the flagging of records which might contain personal information so that such information can be reviewed and removed subject to GDPR policy.

8. HOW LONG WILL WE KEEP YOUR DATA?

The F&FDB does not contain any personal information and so is not subject to the data retention rules detailed in the UK GDPR. The information entered by you into the F&FDB will be stored indefinitely or until RISCAuthority is instructed to cease supporting the F&FDB by its membership.

9. DISCLOSING AND SHARING DATA IN THE F&FDB

We will never sell data from the F&FDB to other organisations. RISCAuthority and FPA will however use and share certain Non-Sensitive data from the F&FDB as detailed in sections 4 and 5.

We may be required to disclose personal information to third parties in order to comply with a legal obligation, or upon a valid request to do so. This may include sharing personal data about individuals with law enforcement bodies, or to help assess fraudulent or potentially fraudulent activity on our systems. These requests are assessed on a case-by-case basis and take the privacy of users into consideration.

10. WHAT ARE YOUR RIGHTS OVER DATA ENTERED INTO THE F&FDB?

Loss adjusters have the right to access, modify and update all case data that they have previously entered on the F&FDB upload site.

Users of the F&FDB have rights over their user account data and at any point whilst we are in possession of, or processing your personal data, you can contact us to enact your rights, as detailed in RISCAuthority's privacy policy (https://www.riscauthority.co.uk/about-us/privacy-policy)

11. WHAT TO DO IF YOU'VE GOT QUESTIONS OR CONCERNS

If you have any questions about the F&FDB that have not been sufficiently covered in this document, or you are unhappy with any aspect of this statement, please contact cford@thefpa.co.uk or call 01608 812500.

Alternatively, you can write to:

Courtney Ford

Fire Protection Association/RISCAuthority

London Road

Moreton-in-Marsh

Gloucestershire

GL56 0RH

If you are unhappy with our response to any requests you have made to us regarding the use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office (ICO). For further information about your rights and how to complain, please visit the ICO website.

If you live outside the UK, you have the right to lodge your complaint with the relevant data protection regulator in your own country of residence.

---------- This Statement was last updated on 29/03/2021 ----------