Information Security Policy

Owner: Chris Martin, Operations Director

Version: 3.5 October 2020

Regulated in the UK by the Institute and Faculty of Actuaries in respect of a range of investment business activities.
First Actuarial LLP is a limited liability partnership registered in England & Wales. Number OC348086.
Registered address: First Actuarial LLP, Mayesbrook House, Lawnswood Business Park, Leeds, LS16 6QY.

Content

1 Introduction

Policy Statement

Information plays an essential role in the business of First Actuarial.

To fulfil our obligations to the data subjects and owners of information, we will ensure the security of this information and the systems on which it is stored, and protect the information and systems from accidental or deliberate damage, loss or corruption.

Objectives

The objectives of First Actuarial's Information Security Policy are to preserve:

- Confidentiality - Access to information shall be confined to those with appropriate authority.

- Integrity – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

- Availability - Information shall be available and delivered to the right person, at the time when it is needed.

Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by First Actuarial by:

- Ensuring that all members of staff are aware of, and fully comply with, the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented within First Actuarial.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

Scope

This policy applies to all full and part time employees, founders, partners, directors and officers, and all consultants and sub-contractors (hereafter collectively referred to as "Staff") working within First Actuarial. All staff are required to ensure that they understand and adhere to this policy and all relevant business procedures.

Failure to follow this policy is a disciplinary offence.

Related Information and policies

The Information Security Policy must be viewed in the context of First Actuarial's overall governance structure; in particular the principles, standards and compliance requirements set out in the First Actuarial Compliance Manual and the Employee Handbook.

The following policies are also related and/or referenced by this policy:

- Cyber security policy – summarises the controls in place to manage cyber security
- Bring your own device policy – sets out policy in relation to staff using their own devices
- Access control policy – details access levels and controls in place

Version

Version	Date	Description	By	Reviewer
3.0	Mar 2018	Original version (2.3) separated into 2 documents, reformatted, and inclusion of more detailed data breach policy	M Sadler	C Martin
3.1	Apr 2018	Updated to reflect comments from the Board	Board	C Martin
3.2	October 2019	Annual review	C Martin	IT, IS reps, DPG
3.3	December 2019	Update to change in password policy, mobile device policy and access controls	M Rowlinson	C Martin
3.4	September 2020	New section on physical security, update for Winzip, add disposal of removal media, note bios passwords, reference cyber security policy and access control policy, clarity on incidents and breaches	M Rowlinson	C Martin
3.5	October 2020	Include multi-factor authentication and meeting client install exemption	M Rowlinson	ITSG

2 Responsibilities for information security

Staff

All Staff have a responsibility to be aware of and to fulfil the relevant security arrangements for their role. We all need to:

- comply with Information Security procedures including the maintenance of data confidentiality and data integrity
- comply with the operational security of the information systems we use
- ensure that the confidentiality, integrity and availability of the information we use is maintained to the highest standard
- report breaches without delay (see Sections 11 to 13).

Failure to comply with the above may result in disciplinary action.

All Staff should inform Chris Martin (Operations Director) if they see ways to improve the Information Security arrangements.

Information Security is managed within First Actuarial by the following:

Board of First Actuarial

The Board of First Actuarial has ultimate responsibility for Information Security including approval of the Information Security Policy.

Operations Director

Responsible for:

- the continuing development and improvement of Information Security;
- ensuring that First Actuarial policies and procedures comply with the ISO27001 standard;
- ensuring that applicable requirements related to Information Security are satisfied;
- driving the review and updating of the Information Security Policy for subsequent approval by the Board. This review shall take place at least annually;
- determining Information Security objectives and appropriate monitoring and measurement arrangements to be able to demonstrate how well those objectives are being met;
- managing Information Security communications and training.

IT Partner

Responsible for:

- managing and implementing the IT aspects of this policy in accordance with any IT policies on a day to day basis;

- leading the IT Strategy Group which has a remit for IT operational matters (including IT aspects relating to Information Security).

Office Information Security Representatives

Responsible for:

- acting as a sounding board on Information Security matters for their local office;
- raising awareness in their local office; for example by running training courses or issuing reminder communications;
- obtaining local feedback, views and suggestions for improvements;
- identifying information security weaknesses and events;
- providing guidance to local employees to help with adherence to respective policies;
- carrying out ISO27001 internal audits and periodic checks on compliance with this policy;
- liaising (with other representatives) to discuss Information Security matters, with the aim of identifying changes/improvements.

Line Managers

Responsible for ensuring that the staff under their management are aware of:

- the Information Security policies applicable in their work areas;
- their personal responsibilities for Information Security;
- how to access advice on Information Security matters.

Data Protection Group

Responsible for:

- acting as a point of reference for all data protection issues in the Firm to help ensure that the Firm is compliant with the requirements of the Data Protection Act 2018;
- the Firm’s breach handling processes including monitoring compliance of it, and reviewing causes of any breaches to identify any actions that may reduce future events;
- providing support on data protection issues in connection with legal agreements with clients and suppliers (in particular ensuring that where external suppliers require access to First Actuarial’s systems, terms of access will be covered by a contract that must be in place before such access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.)

3 Information classification and handling

Types of information

First Actuarial handles the following types of information:

Public - Information intended for public use, eg external website and marketing material.

Internal Firm Information - Internal information that does not contain any client information or personal data. This may include draft 'Public' information that has not yet been published.

It also includes internal processes and procedures.

Client Information - This includes most normal client work, that does not contain personal data.

Personal Data - This is information that contains personal data.

Security Classification

Information is classified to one of three security levels:

Public

Public information is not confidential and does not need to be protected.

This includes all public information. It may include internal firm information that has been explicitly marked as something we are willing to share.

Internal

Information that needs to be protected against external disclosure.

This includes all non-restricted client information and internal firm information.

Information classified as "internal" may be subject to specific additional security measures.

Restricted

Information in this category is subject to the highest security measures.

All Personal Data will fall within this classification.

Client information on particularly sensitive or confidential matters (eg changes to scheme design, advice on redundancy exercises and any mergers & acquisition work) will be classified as restricted. Other client work may be classified as restricted at the discretion of the client manager.

4 Physical security

General office security

All offices have standard key locks and electronic fob access (with some offices also having additional intruder alarms). Fobs are required to access the office at all times and doors are locked manually overnight (and, where fitted, also alarmed overnight.

Fob access is generally restricted to working hours with some tolerance and failed swipes are notified to the IT Team.

Some office parks also include 24 hour security.

Communication room security

All server and networking equipment is situated in a separate room in each office. This room is locked and requires a further electronic fob swipe to enter.

Only the IT Team and a few nominated individuals locally in each office have fobs enabled to access communications rooms. Additionally, all access is expected to be notified to the IT Team in advance of entry, as access of any member of staff (or a failed entry) is automatically alerted to the IT Team.

Access by external parties

Where external suppliers need access to offices they will be supervised.

5 System/Domain security

Locking computers

- All computers (laptops and desktops) should be password locked when unattended (eg at lunch-breaks, comfort breaks and similar).
- Staff must log out and shut down their computer when leaving the office for the evening/over the weekend.
- Staff working remotely who access the network via LogMeIn must sign out when they have finished working for the day.

Windows Password Policy

- Passwords expire and must be changed at least every 180 days. Automatic reminders are issued as expiry approaches.
- Passwords may not be reused.
- Passwords must be meet complexity requirements:
    - Must be at least 10 characters long.
    - Must contain at least three of:
        - English uppercase character (A-Z).
        - English lowercase character (a-z).
        - A digit (0-9)
        - A punctuation mark/symbol.

      But use of all 4 is actively encouraged.
    - Should not be commonly used and obvious passwords (ie not to be based on easily discoverable information).
- Users are responsible for the security and confidentiality of their password. Passwords are:
    - Not to be disclosed or shared with others.
    - Not to be written down.

Account Lockout policy

- Accounts will be locked after multiple (10 in any 30-minute period) unsuccessful logon attempts.
- Accounts will be automatically unlocked after 30 minutes

Multi-factor authentication

- All staff domain accounts will be protected by multi-factor authentication

Password Resets

- Expired or forgotten passwords can only be reset by the IT Team.
- Any such reset must be authorised by a Line Manager before the IT Team implements the request.

Software Installs and updates

- Most staff are prevented from installing software or updates to software which require administration rights. Any such updates will normally be done by the IT Team.
- Staff should not download or install any software even if they are able to do so eg where administration rights are not required. The only exception to this policy is in respect of certain meeting/webinar software which require a client to be installed to use. A list of such software and relevant web addresses will be published on the company intranet, any systems not on this list will continue to need approval from the IT team.
- In specific circumstances, some staff may for operational reasons have administration rights to install software. If a staff member has such rights, how they are used must be agreed with, and permission to install any software sought from, the IT Team in advance.
- Non-business related software must not be installed or downloaded on First Actuarial computer (ie desktops or laptops) hardware.

Use of Peripheral Equipment

- Peripheral equipment (eg a powerpoint clicker or mouse) should not be plugged into First Actuarial hardware unless supplied and/or approved by the IT Team.
- In particular, non-First Actuarial supplied USB devices must not be plugged into USB ports on First Actuarial hardware (only pre-encrypted First Actuarial USB sticks can be written to and used).

Access to First Actuarial systems

The business will ensure appropriate procedures are in place for granting and removing access to all systems. Details of these are included in the Access control policy.

Where staff are absent for longer than 2 weeks (including sickness, maternity/ paternity or other long-term absence) the business may look to restrict access to systems.

6 Electronic data transfers

Physical movement or transmission of electronic data outside of the First Actuarial network, particularly over the public internet or other external networks, is vulnerable to loss, theft or unauthorised access.

Sending Information by Email

All ‘Restricted’ information that is sent by email, outside of the First Actuarial domain, must be contained in a password protected or encrypted attached file.

More specifically:

- Personal member data should not be sent in the open text of an email.
- Member data should be contained in a file of a suitable software package.
- Files containing sensitive and/or personal member data should routinely be zipped and encrypted. A suitable software package will be installed on every user’s PC to either directly zip and encrypt files added into an email as an attachment when selected or zip and encrypt before adding to an email.
- Where recipients (outside of First Actuarial) do not have Zip software (and hence are unable to unzip and open password protected files), the native files (eg Excel files/Word documents/PDFs) should be password protected using the inbuilt security of the relevant software package
- Passwords must be notified to the recipient by another method (eg verbally by telephone, or text message).
- The format of passwords for encrypting should be client specific and contain, as a minimum, a combination of letters and numbers. If an agreed password is reused for client communications it must be updated periodically (for example, when a member of staff who knows the password leaves).

Data on DVD, CD or USB sticks

DVDs / CDs

- ’Restricted’ information that is stored/saved to portable media must be encrypted.
- Encryption should be undertaken using Zip files or native document encryption (Word/Excel/PDFs).

USB Memory Sticks

- Black pre-encrypted USB memory sticks are for internal use only and should not be used to send data externally. If data needs to be sent externally, the IT Team should be contacted for assistance.
- All First Actuarial laptops and desktops are configured so that the USB sockets will not write to unencrypted USB memory sticks (although data can be read from unencrypted USB memory sticks).
- Any USB memory sticks received from third parties should be sent to the IT Team for virus checking and data retrieval from the memory stick.

- Portable media storage containing ‘Restricted’ information should not be left unattended.

When sending portable media storage containing ‘Restricted’ information through the post:

- Recorded Delivery, by an approved supplier or Royal Mail, must be used so delivery can be tracked.
- This must be password protected. The password must not be posted within the same package containing the portable media storage.
- The recipient of the data must be contacted separately to confirm receipt and to be provided with the password to decrypt the encrypted files.

7 Electronic data storage

Whilst it is accepted that data will sometimes need to be stored on their laptop or desktop, staff should aim to minimise the amount of Restricted data stored directly on their machines. All Restricted data should be saved in file shares such as P drive or X drive and copies taken only when needed for offline access.

For desktop machines that are only used in a First Actuarial office, there shouldn’t be a need to directly store any Restricted data directly on the desktop machine.

This will help minimise the risk of loss/inappropriate disclosure of data should equipment be stolen and also ensure data is available to all staff that need it.

Data encryption

Laptops will all be configured to include data encryption on drives via BIOS passwords or BitLocker to ensure all data is encrypted should the device be lost or stolen.

8 Mobile devices

Laptop users

Laptop users present a greater risk to data integrity as a result of the hardware, potentially containing sensitive data, being physically moved outside of First Actuarial's offices.

Laptops must not be left unattended in public places (eg coffee shops, restaurants etc), and laptop users should be vigilant against potential theft of the equipment when outside of First Actuarial offices.

Laptops left in First Actuarial offices overnight must be put away in locked drawers/cupboards or secured to the desk/docking station using a Kensington lock.

Laptops should be shut down before leaving the office, instead of continually being placed into stand-by/sleep mode so that updates can run on shutdown/start-up.

Company provided mobiles/tablets

First Actuarial provides mobile phones to Founders, Partners and some senior staff which synchronise with the First Actuarial network; particularly in relation to emails, contacts and calendars.

All such devices must use a password/PIN number to protect against unauthorised access to the phone/PDA/tablet and/or SIM card.

Own mobiles/tablets

Staff may use their own devices for limited access to FA systems and subject to agreeing to certain conditions of use. These are set out in First Actuarial's Bring Your Own Device Policy.

Use of Public WiFi

The tethering facility on company provided smartphones must be used where possible.

Encrypted WiFi should be used over unencrypted WiFi wherever possible.

However, even encrypted WiFi is not a 100% secure technology so, when using any non-FA WiFi, staff should be vigilant to the potential for websites to be "spoofed" by an attacker intercepting traffic. Staff should be particularly wary of:

- Any web addresses that look odd
- Any SSL certificate errors
- Providing any data to websites using a non-secure connection (anything that starts http rather than http**s**)

9 Disposal of hardware/removable media

All First Actuarial hardware must be returned to the IT Team for secure disposal.

Where multi-functional photocopiers (which have an internal hard-drive) are replaced, instruction should be given and confirmation sought from the supplier that the hard-drive has been wiped/destroyed.

The use of removable media should now be very limited and so should also be returned to the IT Team for secure disposal.

10 Paper based/physical data

Clear desk policy

Non-First Actuarial staff may enter the offices outside of normal office hours; these individuals may include, for example, employees of contracted cleaning firms, or external companies servicing our equipment.

To limit the opportunity of personal information being readily accessible, staff must operate a clear desk policy as described below.

During the day

- When away from your desk ensure that ‘Restricted’ information cannot be accidentally read by others, by closing the file or placing the paperwork face down.
- If ‘Restricted’ information in the form of paperwork or files is being passed to other staff within the office, staff should check that they are in the office that day before leaving this on colleagues desks. Where staff are not in the office, the paperwork or files should be stored securely out of sight until the colleague is back in the office.

At the end of the day

- All ‘Restricted’ information must be removed from desks and stored out of sight in locked cupboards and drawers, or locked filing rooms/racks, with keys then being securely located (ie not left in the locks).
- ‘Internal’ information may remain on the desk but should be in a closed file or face down to prevent accidental reading.
- Barclays internet banking cards should be locked out of sight in lockable cupboards or drawers.

Offsite storage and scanning

Any offsite storage/archive/scanning must only be carried out by a supplier from First Actuarial’s Preferred Suppliers List.

Sending files externally

Where files (or other paper based data) are being transported externally, a courier firm from First Actuarial’s Preferred Suppliers List must be used.

Recipients of information sent by this distribution method must be asked to acknowledge receipt.

Taking files offsite

’Restricted’ information should not, in the normal course of events, be taken offsite, but should be kept in the relevant office.

Where staff need access to paper-based ‘Restricted’ information, such as member data, photocopies of the relevant pages should be taken and these copies can then be taken offsite, provided that they are returned or disposed of after use in the confidential waste bins kept onsite.

Such ’Restricted’ papers must not be left unattended in public places.

Using paper files at home/offsite

Staff who have a business need to take ’Restricted’ information offsite must ensure that such information is not left in plain view. Any such papers should be stored out of sight when not in use.

Any such papers should be returned to the office at the earliest opportunity.

Disposing of data

Any papers containing ‘Internal’ or ‘Restricted’ information which are no longer required should be returned to the office for shredding or disposed of in the confidential waste bins provided, to then be shredded by the relevant external company.

11 Information Security Incidents and General Incidents

Any member of staff who becomes aware of any general incident, information security incident and/or loss of IT equipment must inform their local information security representative immediately. If their local information security representative is not available, they should inform one of the following:

- Information security representative in another office;

- Local Founder or Partner;

- Founder or Partner in another office; or

- The IT Team

Contact numbers can be found on f1rstnet.

What is the difference between an information security incident and a general incident?

An information security incident or general incident includes:

- Disclosure to the wrong people (internal or external). This includes both actual disclosure and potential disclosure (that is, lost data which may or may not have been seen)
- Integrity: Where data is incorrect (either due to a deliberate change or failure to raise knowingly incorrect data)
- Availability: Where data is unexpectedly unavailable

Information security incidents and general incidents apply for both paper and electronic records.

Information security incident

An information security incident has the same meaning as a personal data breach. Under GDPR, a personal data breach means a:

breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

An information security incident is, therefore, a type of incident that involves personal data.

General incident

A general incident arises where internal processing that is carried out does not comply with the Information Security Policy. In most cases, a general incident will not involve personal data, and where personal data is involved, it will not be personal data relating to a client.

In determining whether an information security incident or a general incident has occurred, you should consider the following:

- Is any personal data involved?
- Is it client personal data?
- Is the recipient of the unauthorised information an employee of First Actuarial?
- Has control or access to the information been lost?

Examples of information security incidents

- Device loss
  - Loss of any portable data storage device on which personal data is stored

- Data theft
  - Theft of data by any employee or contractor
  - Hacking attack
  - Malware

- System failure leading to loss or corruption of personal data
  - Virus or Trojan attack
  - Servers become encrypted

- Compliance
  - Failure to put in place contracts with subcontractors
  - Data sharing outside of agreed terms in data sharing protocols

- Errors
  - Such as incomplete mail merging, or mis-matching names and addresses resulting in incorrect data being sent out or data being sent to the wrong individuals
  - Sending an external email to the wrong recipient
  - Attaching paperwork that is unrelated when picking up printed correspondence
  - Payslips and certificates sent to the wrong recipient
  - Benefit calculations sent to the wrong recipient

- Unforeseen circumstances such as a fire or flood

Examples of general incidents

- Internal server(s) briefly being down
- Overfilling confidential waste bins with paper that may contain personal data
- Unauthorised access of folders on the network
- Computer/laptop not properly shutdown
  - includes computer/laptop being left unlocked/unsecured

- Non-staff roaming the office unaccompanied
- Filing cabinets left unlocked
- Loss of staff key fobs for access to FA offices
- Client’s contact details accidentally shared internally

Personal data: Internal oversharing

From time to time personal data may be shared to other individuals within the firm who may not have needed the data. In such case the data did not leave the control of First Actuarial which reduces the risk to the data subjects concerned. In such cases there is no clear divide between incidents and breaches. However, the following is a guide:

General incidents

- Sending data to the wrong person within the same office
- Not removing personal data where possible when sending cases to technical helpdesk.
- Not following the clear desk policy
- Not locking cabinets at night

Information security incidents

- Sending data to the whole firm
- Sending data on multiple data subjects (eg. A spreadsheet) to individuals in another office

In practice, we expect the following to serve as a guide when sharing data internally:

- IT – no data
- Technical Team – no data unless there is a justifiable reason for sending data
- Between teams (for example, IFE and Investment) – data can be shared but consideration should be given to what is being shared.
- Between offices or within offices - data can be shared but consideration should be given to what is being shared.

Reporting information security incidents and general incidents

Any staff member who becomes aware of an actual or potential information security incident or general incident must immediately notify the known circumstances to the information security representative for their office. If the information security representative is not available, they should notify a local founder or partner; or, if necessary, any founder or partner within the firm. Outside of normal hours contact details of founders and partners may be found on the company website.

Where the information security incident or general incident includes the loss or compromise of IT equipment, the loss must also be notified to the IT Team immediately on 0330 363 8000. This number is manned 8am-6pm Monday to Friday.

Outside of those hours a message should be left on the IT Team’s voicemail. The voicemail system includes an automatic alert to members of the IT Team on the out of hours support rota.

Handling information security incidents and general incidents

If any of the following events listed below occur, we will follow the Major Information Security Incident Process (available on firstnet):

- An information security incident affecting multiple clients
- Unauthorised access to an email account (for example, through phishing) and personal data has been obtained
- Unauthorised access to our servers that leads to a loss or corruption of personal data

Otherwise for anything else, the information security representative (or their alternative if they are not available) will determine if the information security incident involves Personal Data. Where information security incidents involve Personal Data, they must follow section 13, otherwise they must follow section 12 for all general incidents.

12 General Incidents

This section concerns general incidents that do NOT include Personal Data going outside the firm.

Investigation and external reporting

The local information security representative shall be responsible for the following:

1. Recording the general incident on the internal Improvements Log.
2. Investigating the general incident.
3. If the general incident involves personal data:
    - Inform the Data Protection Group by email.
    - Inform the client manager. The client manager will then decide what information to report to the client.
4. Deciding what factors gave rise to the general incident and recommending changes to processes or systems to prevent a similar incident in future.

Review of general incidents

The Data Protection Group will review all general incidents recorded on the Improvements Log (including any Personal Data breaches) to establish any changes to procedures that are required across the business.

13 Information Security Incidents - Notification Procedure

About the obligation to report information security incidents

This section concerns information security incidents relating to Personal Data only.

Broadly, Personal Data means data relating to a living individual who can be identified from that data.

First Actuarial must investigate any potential information security incidents that involves Personal Data security breach and identify actual information security incidents.

In some circumstances where an information security incident is likely to have a significant impact, the data controller must decide whether it is a breach of Personal Data. In such cases, it must be reported to the Information Commissioner's Office (ICO) within 72 hours of the data controller being reasonably sure that a breach has taken place.

When a breach of Personal Data security presents a high risk to the rights and freedoms of data subjects, there is an additional duty on the data controller to communicate the details to the individuals concerned so that they can take steps to protect themselves.

Failing to notify a breach of Personal Data when required to do so can result in a significant fine (up to 10 million Euros for a firm of First Actuarial's size).

Investigation and external reporting

The local information security representative and the client manager shall be responsible separately or jointly for the following:

1. Deciding if an information security incident involving Personal Data has occurred
2. Reporting all information security incidents to the data controller.
    - Where the data controller is the client, this should follow any agreed reporting process. If there is no such agreement reporting should be done immediately.
3. Recording the information security incident on the internal Improvements Log.
4. Inform, by email, the Data Protection Group
5. Investigating the information security incident (using the Information Security Incident checklist).
6. Complete the Information Security Incident Report.
7. Where we are the data controller then if appropriate report to the ICO, after using the "Risk Matrix (individual)" to determine the significance of the information security incident, and whether it constitutes a breach of Personal Data as defined under GDPR.
8. Liaising with external agencies and the press in connection with the information security incident.

9. Deciding what factors gave rise to the information security incident and recommending changes to processes or systems to prevent a similar breach in future.

Which information security incidents are reported to the Data Controller?

Unlike reporting to ICO (see below) there is no discretion in whether to report information security incidents involving Personal Data that the data controller may consider to be a breach. Therefore, all information security incidents must be reported to the data controller (which is likely to be the client and the Scheme Actuary).

GDPR itself requires this to be done “without undue delay” and the associated guidance defines this as “promptly.”

On becoming aware of an information security incident, unless otherwise agreed, First Actuarial will report such information security incidents to the data controller within 24 hours.

Which breaches are reported to the ICO?

Decisions on reporting Personal Data breaches to the ICO must be made by the data controller. Depending on the appointment, the data controller may be the client, the Scheme Actuary, or First Actuarial. Our standard appointments allocate responsibility for reporting to ICO to the client.

Guidance from the Article 29 Working Party (advisory body on data protection to European Commission) in 2017 about Personal Data security breach reporting under GDPR is as follows:

“You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.”

When to report to data subjects

Under GDPR there is a duty to report security breaches that are likely to result in a high risk to the rights and freedoms of individuals.

The term ‘high risk’ indicates that the threshold for notifying data subjects is higher than for notifying the ICO.

First Actuarial’s Information Asset Registers for each dataset contain a risk matrix to help determine the level of risk to a data subject in the event of a breach. This should be referred to when deciding whether to report to the ICO or the data subject.