Inspiring Futures Through Learning

Data Protection Policy

Valid From: December 2018
Review Date: April 2019

At Inspiring Futures through Learning, we are driven by our pursuit of excellence every day. We have high expectations of learning, behaviour and respect for every member of our community. We create independent, articulate thinkers and learners who have confidence in, not only their individual ambitions, but also those of the Academy and The Trust as a whole. We have collaboration at the heart of everything we do and our vision is to nurture exciting, innovative, outstanding Academies who embrace change and provide a world-class education for all it serves.

Scope: IFtL Multi-Academy Trust (MAT) & Academies within the MAT	
Version History: V1 – February 2018 v1.1 – December 2018 – post GDPR amendments. For full review April 2019.	**Filename:** IFtL – Data Protection Policy
Approval:	**Next Review on or before:** **April 2019**
Owner: IFtL Trustees	**Union Status:** Not applicable

Policy type:	
Statutory	Website compliancy – required to publish

Data Protection Policy

Introduction

In order to operate efficiently IFTL [the Trust] has to collect and use information about people with whom it works. These people may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

The Trust is committed to ensuring personal information is properly managed and that it ensures compliance with all current data protection legislation including the Data Protection Act 2018 [DPA] and the GDPR.
The Trust will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

1. Scope

This policy applies to all employees, governors, contractors, agents and representatives and temporary staff working for or on behalf of the Trust.

This policy applies to all personal information created or held by the Trust in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

For the purposes of this policy, any reference to the Trust includes the trust offices and all schools that are a part of the trust plus the MKTSA and ITT Teaching Schools.

The DPA/GDPR does not apply to information about deceased individuals.

2. Responsibilities

The Board of Trustees has overall responsibility for compliance with the DPA and with GDPR.

The Data Controller, under data protection law, is Inspiring Futures Through Learning (also referred to within this document as IFtL or the trust). Individual schools are also Data Controllers and share this role, and its responsibilities, with the trust.
The Head teachers of individual schools are responsible for ensuring compliance with the DPA, GDPR and this policy within the day to day activities of their Schools.
Headteachers should appoint a data lead who will be the main point of contact in school for the trust's Data Protection Officer.

Head teachers are also responsible for ensuring that any staff involved in the handling of personal data are trained in the correct procedures and are fully aware of polices relating to data protection.

Although members of staff or contractors who hold or collect personal data are responsible for their own compliance with the DPA and GDPR, schools should ensure that all appropriate technical and organisational measures are in place to ensure that data security is robust and that there is no opportunity for a rogue member of staff to illegally obtain and remove personal data.

Contractors that process data on the organisations behalf must have contracts with the organisation in place that explicitly state that they are compliant with the requirements of the GDPR and that their data security is appropriate.

The Trust's Data Protection Officer is responsible for appropriately advising schools and staff on the correct procedures and their obligation to comply with the legislation, to provide training opportunities to staff that require it, to monitor compliance with the legislation and to advise on corrective actions where appropriate, to conduct internal data audits and to be the main point of contact with the regulatory authorities.

3. The Requirements

Article 5 of the GDPR states that personal data shall be:

- "Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date. Every reasonable step must be undertaken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

- "the controller shall be responsible for, and be able to demonstrate, compliance with the principles"

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual, but need not be sensitive information. It can be as little as a name and address. Such data can be part of a computer record or manual record.

4. Notification

Under data protection law, every data controller who is processing personal data is required to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the trust is registered.

The trust will review the Data Protection Register (http://www.ico.gov.uk/ESDWebPages/search.asp) annually, prior to renewing the notification to the Information Commissioner.

5. Privacy Notices

Whenever information is collected about individuals they must be made aware of the following:

- The identity of the data controller, e.g. the Trust;
- The purpose for which the information is being collected;
- The lawful basis for collection of that information;
- Any other purposes that it may be used for;
- Who the information will or may be shared with; and
- How to contact the data controller.

This must be at the time that information first starts to be gathered on an individual. Privacy notices are displayed in our schools and on our school websites.

6. Lawful Basis for Processing

Under the terms of the GDPR, data controllers must have a valid lawful basis in order to process personal data. The following bases are the grounds on which information is processed within IFtL.

'Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' or 'Necessary for compliance with a legal obligation to

which the controller is subject' - This is the basis for processing general data on pupils of the schools within our trust. As a provider of public education, we are required by law to collect and process personal data on our pupils as without this data, we would be unable to provide and monitor pupils education.

'Necessary for the performance of a contract with the data subject' - This is the basis for processing staff data as without the data we would be unable to pay staff or monitor their performance.

'Necessary to protect the vital interests of a data subject or another person' – This is the basis under which certain pupil data, particularly with regard to safeguarding and child protection, is collected and processed.

'Necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment and social security and social protection law' – This is the basis that certain special category information is collected where such information is required in order to allow schools to fulfil their obligations to look after children in-loco-parentis, particularly with regard to data concerning medical information.

Data that is gathered under any of these bases should only be used for the purposes covered by the basis stated. Data obtained using the public interest basis, for example, should not be used for marketing as the act of marketing is not a task carried out in the public interest. Marketing is likely to require consent, which should be obtained following the principles stated in section 17 of this document.

Any data that does not fall within the categories above must only be obtained after obtaining explicit consent as covered in section 17 of this document.

7. Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- *other members of staff on a need to know basis;*
- *relevant Parents/Guardians;*
- *other authorities if it is necessary in the public interest, e.g. prevention of crime;*
- *other authorities, such as the LEA and schools to which a pupil may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information) or to the DfE where required by law*

The Trust should not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt or statutory requirements conflict, further advice should be obtained.

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled. If there is any doubt, do not disclose the information and seek further advice.

8. Data Subjects and Their Rights

Under the GDPR, Data Subjects have more rights than they had under the previous Data Protection Act. These rights, and how we deal with requests under these rights, are detailed within this section. If there is any uncertainty around the rights of the data subject or if further clarification is required following any communication regarding a person's rights, please contact the trust's data protection officer.

Right to be informed

The right to be informed encompasses the organisations obligation to provide 'fair processing information'. At IFtL, we communicate this by means of privacy notices that are available at our schools and also via our website.
These notices include details such as why we need the data that we are collecting, the lawful basis for processing this data, whether this data is shared with third parties, the retention period for the data, confirmation of the rights of the data subject, a statement about the right to complain to the supervisory authority and the contact details of the trust's data protection officer.
This information must be provided at the time the data is collected if it directly obtained from the data subject or within 1 month of collecting the data if it is not obtained directly from the subject.

Right of access

Individuals have the right to confirmation that their data is being processed, the right of access to their personal data and the right to other supplementary information (generally, this refers to the information that should be provided in privacy notices).
This information must be provided to data subjects free of charge. A fee, however, may be charged if a request is manifestly unfounded, excessive or repetitive.
Information, following subject access requests, must be provided without undue delay and, at the latest, within 30 calendar days.

Further guidance on how to deal with subject access rights follows at the end of this section.

Right to rectification

Individuals have the right to have any incorrect or inaccurate personal data rectified. This means that, where a request has been made, all records relating to that individual, where information is found to be incorrect, must be corrected within 30 calendar days. This relates to paper records, computer files, backups of computer files and, where possible, records kept by third parties where the information has been passed on by the trust.
Requests can be extended by 2 months where the request for rectification is complex.

Right to erasure

The right to erasure is also known as 'the right to be forgotten'. This is to enable an individual, where it is appropriate, to request the deletion or removal of personal data relating to them where there is no longer a compelling reason for its continued processing.

It is important to note that this is not an absolute right and the right of erasure can be refused in many circumstances.
Where data is no longer necessary in relation to the purpose for which it was originally collected, where an individual has withdrawn consent, where an individual objects to the processing of their data and there is no overriding legitimate interest for the continued processing of the data or where data is being unlawfully processed are some of the reasons where the right to be forgotten may be upheld.
Any case where a data subject requests to exercise this right should be referred to the trust's data protection officer.

Right to restrict processing

An individual can request that their data is no longer processed, that is, no longer used by the organisation. If this happens, the organisation retains the right to store the data, but may no longer further process it. This restriction may happen if the accuracy of data is contested, where an objection has been made against the processing, where processing is unlawful and the data subject requests restriction rather than erasure of data or where the organisation no longer requires the data but the individual requires the data to be retained in order to establish, exercise or defend a legal claim.
If this data has been passed on to third parties, there is an obligation to pass the restriction details on to them unless it is impossible, or would involve disproportionate effort, to do so.

Right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This right should allow them to move, copy or transfer personal data easily from

one IT system to another, safely and securely.
Data should be supplied in a structured, commonly used, machine readable format (An example of this format would be a .csv file) where possible.
This information must be provided free of charge within 30 calendar days.
There is no obligation to make data compatible with a proprietary format nor to convert paper records to electronic format.
This right is unlikely to be exercised within a school setting and is primarily aimed at businesses and financial institutions. Schools, however, should be aware of the right and of its implications.

Right to object

Individuals have the right to object to their data being processed based on legitimate interest or the performance of a task carried out in the public interest. They also have the right to object to direct marketing, including profiling and to the processing for purposes of scientific or historical research and statistics.

Where data is being processed on legitimate grounds, individuals must have an objection based on grounds relating to their own 'particular situation'. You must stop processing the data unless you can demonstrate compelling legitimate grounds for the continued processing which override the interests, rights and freedoms of the individual or unless the processing is for the establishment, exercise or defence of legal claims.
Individuals must be informed of the right to object 'at the point of first communication'. This right is stated in our privacy notices and should be explicitly brought to the attention of the data subject.

Rights related to automated decision making, including profiling

Individuals have rights with regard to automated decision making (where no human involvement is included in the making of a decision) as well as automated profiling (where personal data is analysed to evaluate certain things about an individual).
Currently, neither the trust nor its schools undertake any automated decision making or profiling. Should any automated systems be investigated in the future, a data protection impact assessment should be undertaken prior to any systems being put into place.

Further guidance on subject access requests

Any person whose details are held by the Trust is entitled, under the GDPR, to ask for a copy of all information held about them (or child under 13 for which they are responsible).

The first step to take when dealing with a subject access request is to establish the identity of the person making the request and ensure that they are entitled to receive the information requested. Parents must have parental responsibility over a child in order to be eligible to request information.

Data provided must be in an intelligible format with an explanation of any terms that are not understandable without an explanation (such as internally used acronyms or abbreviations). Information should be provided, where possible, in a 'commonly used electronic format' unless otherwise requested by the individual. When providing the information the School must also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

Responses must be made within 30 calendar days and no charge can be made for the provision of the information unless the request is 'manifestly unfounded or excessive' in which case, a charge can be made or a request ca be refused. No definitions, however are given of the terms 'manifestly unfounded' or 'excessive'. Organisations must be able to provide evidence of why the request was considered such if either of these reason are used.

Schools should refer to the trust's data protection officer for advice before dealing with any subject access requests.

Schools will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

9. Provision of data to children

Under GDPR, the age at which a child can give their own consent to process data is 16. The 2018 DPA has lowered this, in some circumstances, to 13. Currently, all schools within the trust are primary therefore further consideration to consent or requests relating to children have not been included within this policy. Should the trust acquire a secondary school, this policy will be reviewed to include this provision.

10. Parents' rights

The Education (Pupil Information)(England) Regulations 2005, do not apply to academies and free schools, therefore a parent's right to access their child's educational record does not apply within the IFtL trust as long as an annual report on the child's progress is provided.
Schools may decide, on a case by case basis, to grant a request to access a pupil's educational record and will bear in mind any guidance issued from the ICO.

11. Information Security

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).
The requirement of GDPR is that only people with a legitimate entitlement to access data should be allowed to do so, therefore any paperwork containing personal data should be locked away at the end of each day or offices should be locked so that persons that are not authorised to access the data are unable to do so.
Computer screens must also be locked whenever an employee leaves their workstation in order to protect any data that is accessible from that workstation.
Portable flash drives (USB sticks) should not be used, under any circumstances, for the storage of personal data. These devices are easily lost or corrupted. (The use of such devices for non-personal information is acceptable, although all staff should be working from the IFtL Sharepoint Portal which should reduce the need for portable drives).
Laptops or tablets, where they have access to personal data, should be password protected and drives should be encrypted to minimise the risk of a data breach in event of the loss of a machine.
Schools should ensure that administrator password to networks are kept secure and only provided to persons that absolutely require access. Where possible, access should be restricted to only the areas required and each administrator should have their own password so that access can be easily revoked if required.
Schools should consider penetration testing and ethical hacking services in order to assure the security of their networks.

12. Maintenance of up to date data and disposal of data

Personal data should be checked and updated at appropriate intervals. Staff and parents should be given the opportunity to check relevant personal data and make corrections on a regular basis.
The sending out of pre populated data collection sheets is something that should be avoided. Putting a sheet full of personal information in the post or in a child's book bag, for a parent or carer to review is, in itself, a potential data breach. Sending out a blank form is acceptable and the data on the returned, populated form then becomes the responsibility of the parent/carer.
A better solution is to review the forms with the parent/carer at a parents evening. This helps to ensure the data is secure as it does not leave the building. (Bear in mind that these sheets should then be returned to their designated location and locked away prior to staff leaving the building).

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. The attitude where data is kept 'just in case' should be avoided. In reality most relevant information should be kept for the period during which

the person is associated with a school plus an additional period determined by the records management policy. Ideally, where data is archived, a disposal date should be clearly marked on boxes or folders.
When it is time for data to be disposed of, it should be destroyed in an approved manner. For paper records, this will be by use of a cross cut shredder or by means of a contractor who is a member of the UKSSA or the NAID and, ideally, accredited to BS EN 15713.
Where electronic information is disposed of, this must be done under contract with a supplier where the contract assures that the terms of the GDPR are complied with. This extends to disposal of any computer equipment containing storage media (hard drives etc) that may have processed personal data during the lifetime of the equipment.

Schools should maintain a data asset register listing what data they hold, where it is held, who has access, why they have this data and for how long the data is kept. This can be a modified version of the data audit carried out by all schools and departments during the lead up to GDPR. This asset register should be updated as systems and data change.

13. Inaccurate Data

Under GDPR, data subjects have the right to rectification, the right to erase, the right to object and the right to restrict processing.
This means that data subjects can ask for their data to be corrected where it is inaccurate or incomplete, erased under certain circumstances, although this right is not absolute and there are many grounds for refusing the right to erasure, they have the right to object to the use of their data and they can also request that their data is no longer processed.
Should schools receive any of these requests, please refer to the trust's data protection officer.

14. Recording of Data

Records should be clear, concise and accurate. It should also be borne in mind that at some time in the future, the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

15. Photographs

Photographs are considered personal data and require the same protection as any other type of personal data.

Collecting photographs for use on SIMS will fall under the public interest basis so consent is not required. Photographs used for other purposes, however, will most likely require consent..

Consent under GDPR is required to be unambiguous, specific and freely given. This means that blanket consent for photographs is no longer appropriate and consent must be given for each different use required for photographs. Consent must also be opt-in and not opt out. Pre-selected opt in boxes also cannot be used. A consent form should list each reason for consent along with a yes and no box plus a space for a signature following the boxes.
Consent that is given can be withdrawn at any time. This means that, even if consent is given and photographs are used, for example, on a school website, that consent can be withdrawn as soon as they are published, or at any time thereafter, and the data controller has an obligation to ensure that those photographs are removed as soon as possible.
There are some allowances made where it would be costly to the business to withdraw consent, for example, if you have just printed a prospectus and consent is withdrawn for a photograph within it, it may be acceptable to continue to use these but to remove the photograph in future print runs.
If there is any doubt around this, please contact the trust's data protection officer.

17. Further rules around consent

Consent should not, where possible, be used as the basis for processing data as any consent given can subsequently be withdrawn.
Any data that is necessary to perform the tasks required of the organisation by law, should be gathered using the lawful bases for processing detailed in part 7 above of one of the other lawful bases listed under article 6 of the GDPR (or article 9 for special category data).
Where data is required that does not fall within the bases stated, consent should be obtained in order to process this data prior to any processing taking place.
This can include photographs, as in part 16 above, or other data that may fall outside of the scope of the lawful bases stated.
Where consent is required, it must be freely given, unambiguous and explicit. It also requires a positive opt-in which means that pre-ticked boxes or boxes where you must tick to opt out are illegal under GDPR.
The requirement for consent to be explicit also means that consent must be given for each individual use of the data. Using photographs as an example, it is no longer permitted to ask for consent for photographs to be used for 'use on our website, newsletters, within school and other areas' . Each specific use of the photographs must individually be consented to and a dated signature should be obtained to show when consent was obtained and records should be kept.
Individuals should also be informed that they have the right to withdraw their consent at any time and should also be informed if the data that they are consenting to will be passed on to any third parties for processing.

18. Breach of the policy

Non-compliance with the requirements of the DPA/GDPR by members of staff is a serious matter. Fines under GDPR can be up to €20 Million or 4% of annual turnover, whichever is the greater. Staff can also be personally convicted of criminal offences, for example, obtaining or disclosing personal data for their own purposes or without the consent of the data controller can lead to criminal prosecution. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal.

19. Procedure in the event of a data breach

A data breach can be any loss, destruction, unofficial alteration, unofficial access, theft or disclosure of personal data.
Any potential breach of data MUST be notified to the trust's data protection officer as soon as it is discovered.
The DPO will investigate the potential breach with the school and decide what action to take.
Certain breaches are reportable to the supervising authority and that report must be filed within 72hours of the first discovery of the breach. It is critical, therefore, that potential breaches are reported to the data protection officer immediately.
Fines can be imposed by the supervisory authority for infringements relating to breach notification. Potential fines for improper reporting of data breaches fall within the lower band of fine under GDPR, which is 'up to €10 Million or 2% of annual turnover'.

20. Transferring data outside of the European Economic Area

There are certain rules regarding the transfer of data outside of the EEA under GDPR. This includes the storage of data on 'cloud' service providers.
It is unlikely that the trust, or any of its schools, will transfer data outside of the EEA. They should, however, consider the following if this becomes applicable;

Transfers may be made to a third country where the European Commission has declared that the country, or international organisation, provides an adequate level of protection.
Transfers may be made to certain American companies that have adopted the EU-US Privacy Shield.
Transfers may be made to certain companies subject to appropriate safeguards, such as binding corporate rules, compliance with an approved code of conduct approved by a supervisory authority or certification under an approved certification mechanism as provided for in the GDPR.

There may be other conditions under which transfers may be made. In all cases, the trust's data protection officer should be consulted about transfers outside the EEA.

21. Provision of online services to children

Where online services that collect personal data are offered to children, explicit parental consent must be obtained. This is particularly significant where children's personal information is used to create online profiles or for marketing. (Preventative or counselling services do not necessarily require parental consent.)

It is unlikely that these services will be offered by the trust or its schools but schools should ensure that any apps or websites used for educational purposes are compliant with GDPR before putting them to use in the classroom.

22. Use of email and document security

Any personal or confidential data should not, under any circumstances, be sent via email. General email is an insecure system and the potential for data loss or interception is very high.
All staff, governors and trustees should be issued an IFtL email address for their use with regard to work matters. Use of personal email addresses for work matters should be avoided wherever possible.
Where agendas and papers for meetings are issued, these should be hosted on the portal and links distributed by email as opposed to sending out documents attached to an email. This helps ensure the security of the documents and also helps with version control as there will only be one copy of the document in use rather than various copies which may not pick up any modifications made.
Particular attention should be paid to permissions when sharing documents and you should consider whether to send documents with read only rights or whether editing is necessary.

23. DPIAs and Data Protection (Privacy) by Design

It is critical that any new systems take data protection into account at the planning stage. When looking into any new systems that handle personal data, a Data Protection Impact Assessment (DPIA) should be undertaken to ensure that the security, protection and privacy of data held within the new system is assured prior to any purchasing taking place.
For information regarding DPIAs, please see the ICO guidance on Privacy Impact Assessments or refer to the trust's data protection officer.

Further guidance on all matters relating to data protection is available from the trust's data protection officer or from the Information Commissioners Office.

Abbreviations

Abbreviation	Description
DPA	Data Protection Act 2018
EIR	Environmental Information Regulations 2004
FoIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation

Glossary

Data Controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Data Subject	The person whose personal data is held or processed
Educational record	The educational record is confined to information that comes from a teacher or other employee of a local authority or school, the pupil or their parents. Communications about a particular child from head teachers and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record.
Information Commissioner (ICO)	The supervisory authority for data protection in the UK
Personal Data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Processing	Obtaining, recording or holding data

Sensitive Personal Data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence Criminal convictions
Subject Access Request	An individual's request for personal data under the Data Protection Act 2018 or the GDPR.