Producers' Data Protection and Security Guidelines

1. Introduction

These guidelines set out recommended safeguards that all production companies should implement in order to protect personal data including special category data (previously known as sensitive personal data) in the light of the General Data Protection Regulation ('**GDPR'**), effective from May 25th 2018. This is implemented in the UK under the Data Protection Act 2018 ('**DPA 2018'**).

This Guidance is a living document and updates will be issued periodically.

The GDPR is the new European data protection legislation and the DPA 2018 supersedes the Data Protection Act 1998 ('**DPA 1998'**). The implementation of the GDPR is intended to give individuals better control over their own personal data. The GDPR brings with it some new principles and concepts, including new rights for individuals.

These guidelines are designed to provide practical advice to assist producers in protecting personal data and in turn to protect production companies from civil and/or criminal sanctions and reputational damage as the result of loss or damage to, or an unauthorised disclosure of, personal data or special category data.

It is important that all senior staff read these guidelines and that practical support and guidance is provided for all staff within the company. It is recommended that one senior person, Data Manager or a Data Protection Officer takes overall responsibility for data protection policy and practice for the whole company. Contact details of that senior person, Data Manager or Data Protection Officer should be made available and accessible to all staff and anyone who has a query about how the company handles their personal data.

The website of the Information Commissioner's Office (**'ICO'**), the UK's regulatory body for data protection, provides useful information to help with most compliance issues. If you have specific detailed enquiries then the ICO telephone helpline can help to answer these. You may also want to consider if it would be helpful for staff members or those engaged by you to attend a training session or course in order to help them understand your obligations under the GDPR.

Please also see the attached Production Crew Data Security Guidelines which set out practical advice and assistance for your production crews when dealing with living people's personal data and special category data.

2. Who is in charge of GDPR in the UK?

The ICO is responsible for enforcing GDPR in the UK. The ICO has the power to conduct criminal investigations, take enforcement action and issue fines.

3. Do I need to register with the ICO for the GDPR?

If you collect and process personal data it is highly likely that your company will need to pay a fee to register with the Information Commissioner for listing on the Information Commissioner's register. This is a legal requirement and failure to pay a fee to register could result in a fine.

If you needed to register under the DPA 1998, then you will probably need to register and pay the relevant fee under the new charging structure for data controllers contained in the **Data Protection (Charges and Information) Regulations 2018**. This came into effect on 25th May 2018, to coincide with implementation of the GDPR and the DPA 2018. (This does not mean that you had to re-register and pay the new fee on 25th May. Data Controllers who have a current registration (or notification) under DPA do not have to re-register or pay the new fee until their current registration has expired).

ICO guidance on fees for registration can be found here: https://ico.org.uk/for-organisations/register/

4. What does the GDPR apply to?

The GDPR applies to personal data and to processing activities carried out by companies within the EU, as well as companies outside the EU who offer goods or services to individuals in the EU.

5. What is personal data?

There are two types of data: **personal data** and **special categories data**. Special category data is still personal data, but requires further processing conditions (as it is likely you will still require a non special category data condition as well) Please see more below in point 5.2.

5.1 Personal data

Personal data is data which relates to a **living individual** and that can be directly or indirectly linked to that person, or data from which an individual can be identified when the personal data is read in conjunction with other readily available information. This may include **any one or more of** their name, address, images, telephone numbers, personal email addresses, date of birth, bank and pay roll details, next of kin, passport particulars etc. The GDPR's definition of personal data is broad and makes it clear that information such as an online identifier, for example an IP address, can be personal data. Even data that has been pseudonymised can be classified as personal data depending on the ease of attributing that data to a particular individual.

If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and process with this in mind (further information is available at section 12 of this guidance).

5.2 What is special category data?

Special category data (previously known as 'Sensitive Personal data' under the DPA 1998) relates to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, and sexual orientation/life. It also includes genetic and biometric data. Article 9 in the GDPR states that the processing of special category data is prohibited, unless one or more of the lawful bases in that Article can be met. Personal data relating to criminal convictions and offences **are now not** included under this definition but there are similar safeguards for processing (as detailed in section 5.3 of this guidance).

5.3 What is criminal offence data?

The concept of criminal offence data includes data about criminal allegations, proceedings, convictions and offences or related security measures.

There are separate safeguards set out for Criminal Offence Data in the GDPR and these are set out in the GDPR Article 10 and under the DPA 2018.In order to process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.

Production companies may only collect information about criminal convictions if it is appropriate given the nature of the role e.g as part of a recruitment process for the purposes of safeguarding children, and you are legally entitled to carry out enhanced/standard or request a basic Disclsoure Barring Service checks (if for the purpose of safeguarding children you can rely on Schedule 1, Part 2, paragraph 10 and Paragraph 18 under the DPA 2018). Please be aware that for both of these bases there is a requirement to have an appropriate policy document in place, as per Schedule 1, Part 2, Paragraph 5 (1) and Schedule 1 Part 4 under the DPA 2018

Be aware that you cannot keep a comprehensive register for criminal convicitons unless you do so in an official capacity.

Please read the most up to date ICO guidance if you intend to deal with this type of personal data for your programme and if you are unsure seek legal advice and speak with your commissioning broadcaster:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/

6. Where is personal data found?

Your employees and freelancers will have access to or will routinely acquire personal data from many sources and in many forms. For example personal data can be obtained from past, current, and future employees, contributors, suppliers and contractors.

Personal data will be in your programmes, rushes, or provided in letters, emails, correspondence, call logs, programme treatments, running orders, CVs, CCTV footage, contributor agreements or release forms, contributor application forms, call sheets, P-as-Cs, a disclosure & barring service checks, medical records, invoices, purchase orders, rushes with captions, bank statements, lists of employees, from websites and employee references. Personal data may be in **hard copy form** e.g. original or copy paper document, photographs and film; or **electronic form** e.g. PC, laptop, mobile phone, blackberry or memory stick.

When proposing to collect personal data, care should be taken to limit the personal data collected to what is actually necessary.Don't collect peronsal data just in case you might need it. For example, it is unlikely that you would need information regarding a contributor's sexual history, unless it was relevant to the programme.

The definitions for personal data are broad, and you might be processing both special category data and personal data when making a programme.

If you are handling personal data, you need to establish your level of responsibility and this is based on whether you are a data controller or data processor. Whether you are a data controller or a data processor is a matter of fact and is based on whether you determine the means and purpose for the processing of data. An organisation or a company cannot decide their status for the purpose of avoiding certain obligations.

7. Are you a data processor or a data controller?

Data controllers are ultimately responsible for compliance in respect of the personal data and must be able to demonstrate that they comply with the data protection principles (see section 8). Be aware that a production company can be both a data controller and a data processor in regard to personal data or a joint controller of personal data, but it cannot be a data controller and data processor at the same time in respect of the same personal data.

7.1. What is a data controller?

A data controller determines the purposes and means of processing personal data. In some circumstances, where more than one party decides the purpose and means of processing, they are 'controllers in common', or joint controllers. If you are a data controller and you engage a data processor to carry out processing activities on your behalf, the GDPR places obligations on you to ensure your contracts with data processors comply with the GDPR. Under the GDPR the data controller has the responsibility to comply, and to demonstrate compliance with, the data protection principles of the GDPR. For example producers will be data controllers in respect of all personal data processed in the course of developing and producing the programmes they are commissioned to producer unless otherwise set out in writing and agreed between parties.

7.2. What is a data processor?

A data processor iFs responsible for processing personal data on behalf of a data controller. If you are a data processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities and report a data security breach involving personal data to the data controller promptly and without undue delay. You are also required to implement appropriate technical and organisational measures for protecting and retaining personal data. Please note employees are not data processors for a company, if the company is a data controller and an employee is acting on behalf that company they are acting in the capacity as a data controller.

7.3 What if I am engaging a third party to handle personal data for the Programme?

If you are using a third party to collect, process or dispose of personal data on your behalf and this party is not determining the purpose and means of the processing, it will be a data processor.

An example of a processor may be a company you use to run and host an online application forms for programme contributors or a company that provides online contributor release forms that can be signed on location from an iPad.

Your contract with those companies should include;

- the duration of their processing;
- the nature and purpose of their processing; the categories of personal data and data subjects;
- your rights and obligations as a data controller;
- that the data processor will only process data on your instructions
- that the data processor must ensure that the persons authorised by them to process personal data have appropriate confidentiality obligations placed on them;
- that the data processor has implemented required security measures;
- that the data processor can't sub-contract to another data processor without your specific consent and if they do contract another data processor the same obligations are placed on that sub-contractor;
- that the data processor will assist you with appropriate technical and organisation measure for the fulfilment of your obligations to data subjects;
- that the data processor will assist you in complying with your obligations pursuant to Articles 32 to 36 of the GDPR, that the data processor will notify you of a data breach;
- that the data processor will delete or return all personal data at the end of the provision of the services and that you can audit that data processor to demonstrate compliance.

You must ensure that your data processor undertakes to abide by the GDPR. As the data controller you will be responsible for any breaches of the GDPR which arise from the activities of the processor undertaken on your behalf However a data processor will also be responsible for their failure to comply with their GDPR obligations. If a data processor becomes aware of a breach of data security, then the data processor must inform you without undue delay.

Data processors also have direct responsibilities under the GDPR and may be subject to fines or other sanctions if they do not comply.

For example, if a data processor uses a sub-processor then it will, as the original data processor, remain directly liable to the data controller for the performance of the sub-processor's obligations. In addition to its contractual obligations to thedata controller, under the GDPR a data processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer (if necessary).

As a data controller, the GDPR requires you to have a written contract in place with your data processor which contains certain specified terms as set out above.

If a data processor fails to meet any of these obligations or acts outside or against the instructions of the data controller, or its requirements under GDPR, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures issued by the ICO.

Where a data processor is processing personal data that, if lost, damaged or accessed without appropriate authority may cause harm to individuals, to your company or to your commissioning broadcaster in the context of a production, it is appropriate to (i) expressly provide in your contract with your data processor that it must comply with the requirements of the GDPR (ii) include provision in the contract for you to be able to inspect and/or monitor its compliance where practical and necessary and to make available all information necessary to demonstrate their compliance to you.

For more information the ICO has set out what is considered personal data, data controllers and data processors. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/.

8. The GDPR Principles - Policies and Personal

All production companies must have in place an appropriate data protection or equivalent data security policy that sets out how they manage personal data within the company and when making programmes. The policy should incorporate

the **Principles of the GDPR**. These principles are similar to those in the DPA 1998, with a new accountability requirement that a data controller is responsible for and must be able to demonstrate compliance with the principles

All companies must ensure personal data is:-

i. processed lawfully, fairly, and in a transparent manner.

ii. collected for specified, explicit, and legitimate purposes (further processing for archiving, purposes in the public interest, scientific, or historical research purposes, or statistical purposes is not considered to be incompatible with the initial purposes);

iii. adequate, relevant, and limited to what is necessary;

iv. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay;

v. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes; (for longer periods this can be done solely for archiving in the public interest, scientific or historical research, or statistical purposes - subject to appropriate technical measures being in place to safeguard the rights and freedoms of individuals);

vi. ensuring 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.

9. What is a lawful basis under the GDPR?

Under the GDPR you must have a lawful basis in order to process data. The ICO recommends keeping a record of the lawful basis on which you have relied for each processing activity, and an explanation of why it applies. Your lawful basis should be communicated to the data subjects as part of your privacy notice and/or privacy policy at the time of collecting the personal data.

The first principle of the GDPR requires all personal data to be processed lawfully, fairly, and in a transparent manner. If there is no lawful basis for the processing, the processing will be unlawful and in breach of the first principle.

You should review the basis on which you are processing personal data under the GDPR, compared with the previous basis under the DPA 1998. You may decide that a different basis under the GDPR is more appropriate (see section 10). If processing for a new purpose has a lawful basis, you will still need to consider whether processing for the new purpose is fair and transparent.

ICO guidance can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

ICO has introduced an interactive tool to help you identify the relevant lawful basis: https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/

10. Lawful bases in which you can handle personal data.

There are 6 lawful bases to choose from. Each lawful basis will have an effect on the rights of the individual. Except in respect of consent, you may apply more than one lawful basis, in which case you should identify and document all of them as early as possible. If you are applying consent as the lawful basis there may be seriour consequences for programme making. You should seek legal advice about whether to to rely on consent as a lawful basis for your programme.

The 6 lawful bases are set out and explained below:

10.1 Consent

Under the GDPR, valid consent becomes significantly harder to obtain and therefore it is often not the best basis to rely on for processing an individual's personal data. It's important to note that an individual's consent to processing personal data cannot be conditional on eg, appearing in a programme. It must be freely given and the consent must be able to be withdrawn at any time by the individual. To be able to process data under this lawful basis;

- an individual has to have given **clear** and unambiguous consent for you to process their personal data for the specific purpose for which consent was requested.
- It requires a positive opt in / you should be able to clearly demonstrate how the individual has taken a positive action to indicate their consent; and
- it needs to be able to be withdrawn at any time (and you must inform the individual how they can withdraw it). It should be as easy to withdraw consent as it was for the individual to give it in the first place.

You would rely on consent as a basis for processing where you are marketing to an individual and you should make yourself familiar on the direct marketing requirements of the Privacy Electronic Communications Regulations ('PECR').

Please read the ICO guidance on PECR: https://ico.org.uk/for-organisations/guide-to-pecr/

Producer Note:

Consent will not often be the most appropriate lawful basis for processing in relation to a programme. This is because a person must be able to withdraw consent at any time and this withdrawal of consent would have a significant impact on your ability to deliver your programme to a broadcaster. Therefore where possible you should not rely on consent for the legal basis of your processing, however in the event that there are circumstances where it may be necessary to rely on consent and you are unsure you should seek legal advice.

- Collecting and processing contributor personal data is usually necessary for the purposes of performance of the contributor contract (see section 10.2 below). Consider carefully whether in light of the ability for consent to be easily withdrawn if it is appropriate and/or prudent to rely on consent (or you rely on consent where it is strictly necessary and clarify when consent cannot be withdrawn e.g. once information has been made public by their participation).
- It's important to note there is a distinction between consent for processing of personal data and the requirement to obtained informed consent for participation in a programme as set out in the Ofcom Broadcasting Code which is still required.

10.2 Contract

'Contractual necessity' remains a lawful basis for processing personal data as it was under the DPA 1998. You can use compliance with a contract as a lawful basis if your processing is necessary for the performance of a contract to which the individual is party, or before a contract is entered into, in anticipation of a contractual relationship. You need to ensure that it is necessary, and that you have documented your decision to use this lawful basis and that they have agreed to this lawful basis for processing.

Producer Note:

You should ensure that individuals who are involved/contribute to the making of programmes are contracted under an agreement/ contract and they are aware that this is the lawful basis on which their personal data is being processed in making the programme. It would also be prudent to have a further legal basis to rely on in your contributor agreement/ release form for example, legitimate interest.

10.3 Compliance/ legal obligation

An example of processing in compliance with a legal obligation could be processing someone's bank details and retaining them to comply with HMRC rules or processing information about a contributor's food allergy on a cooking show in order to comply with our Health and Safety obligations. The main change from the DPA 1998 under this lawful basis, is that the GDPR explicitly limits these legal obligations to those arising in under UK or EU law. This may mean that organisations that are subject to a non-EU court order to disclose could put you in a difficult position.

10.4 Vital interests of the data subject

This category may be relied on if you process someone's personal data in order to protect their life, and where the processing involves heath or special category data, this is only in situations where consent cannot be given. For instance, if someone is in need of urgent health care at the hospital and is not in a state to give consent to processing of their data.

10.5 Performance of task in the public interest

The processing is necessary for you to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

10.6 Legitimate interest

Processing carried out on the basis that it is in the 'legitimate interests' of the data controller or others is the most flexible basis for processing; this will be most appropriate where you use individual's data in ways they would reasonably expect and such processing would not have an unwarranted impact on them whilst balancing it against the individuals's interests, rights and freedoms. When processing personal data under this basis you need to take extra care and responsibility for considering and protecting people's rights and interests and document your legitimate interest assessment. You will need to carry out a legitimate interests impact assessment. The legitimate interests can be your own interest or the interest of third parties. They can include commercial interest, individual interest of broader social benefits. However if you chose to rely on legitimate interest you are taking on extra responsibility for considering and protecting people's rights and interests. You will also need to include details of your legitimate interest in your privacy information. However practically it is likely that contractual necessity and compliance as a legal obligation may be more appropriate for your lawful bases.

For further information please read the ICO guidance on legitimate interests:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Producers Note:

A producer must set out their lawful basis before processing personal data. This means setting out your lawful basis before starting to make a programme, or if not possible then you should do so as early as possible. Your lawful basis must be documented, as well as the reason why this legal basis was chosen. You may wish to consider discussing your lawful basis with your commissioning broadcaster, depending on the type of programme you are filming, as there may be more than one lawful basis, for example;

- Setting out your lawful basis when you involve or engage those you are filming with in your programme i.e. this is likely to be performance of a contract. If you were relying on consent a person could withdraw consent at any time and this would have a significant impact on your ability to deliver your programme to a broadcaster. Please see point 10.1 for more information on this.
- Public Filming notices: this would likely be subject to the lawful basis of legitimate interest.
- Secret filming: this would likely be subject to the lawful basis of legitimate interest or journalistic exemption.

11 Processing conditions in which you can handle special category data

Special category data is more sensitive by its nature and needs more protection. This is because this type of data could create significant risks to a person's fundamental rights and freedoms if it were to be subject to a breach or processed incorrectly, e.g by putting them at risk of unlawful discrimination.

The GDPR has provided additional grounds under which this information can be lawfully processed . You must identify a separate condition as well as a lawful basis for processing special category data and these are set out in Part 2, Chapter 2, paragraph 10 as well as in Schedule 1 of the DPA 2018

11.1 Explicit consent: where a person has given explicit consent to use this information, in order to legitimise the processing. Note that some of the other conditions still require you to consider consent first, or to get consent

for some elements of your processing. For example, if you are a not-for-profit body and you choose to rely on Article 9(2)(d), you still need explicit consent to disclose the data to any third party controllers.

Please read ICO guidance on consent:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

11.2 **Employment law:** exercising obligations and rights for employment, social security, social protection law, or a collective agreement

11.3 **Vital Interests**: protects the person where they are physically or legally incapable of giving consent. This is intended to apply to life or death situations where someone is in immediate need of emergency health care;

11.4 **Charity or not for profit bodies:** Where a foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim provided it relates solely to the members or to former members of the body or to persons who have regular contact and that such personal data is not disclosed outside that body without the consent of that person;

11.5 **Data made public by the data subject**: personal information manifestly made public by the individual. This may be relevant for special category data that is included editorially in the programme.

11.6 **Legal Claims:** exercise / defence of legal claims or when courts are acting in their judicial capacity;

11.7 **Substantial public interest:** for reasons of substantial public interest. Schedule 1 in the DPA 2018 sets out several conditions for meeting the substantial public interest requirement which includes for the purposes of a function conferred by an enactement or rule of law, such as an obligation under Health and Safety law. You will need to satisfy at least one of these conditions in Schedule 1. This has to be proportionate to the aim pursued and respect the right to data protection whilst at the same time providing for suitable and specific measures to safeguard the fundamental rights and the interests of that person.

11.8 **Medical diagnosis and treatment:** for preventive / occupational medicine, for assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment or the management of health or social care systems/ services or to contract with a health professional.

11.9 **Public health:** such as protecting against serious cross-border threats to health, ensuring high standards of quality and safety of health care/medicinal products or medical devices, ensuring safeguard of the rights of the individual and professional secrecy;

11.10 **Historical, Statistical, or Scientific:** for archiving in the public interest, scientific or historical research or statistical purposes proportionate to the aim.

Producer Note:

Producers are likely to rely on a number of the above conditions alongside the lawful basis such as necessary for performance of a contract and/or legitimate interest. You must identify both a lawful basis and one of the above conditions in order to process special category data. You may, for example, use special category data in the following circumstances;

- Information you gather for employment purposes, or use collective of arrangements for payment of residuals/royalies..
- For programmes, you may include special category data iwhich has already been manifestly made public by that person,
- Conducting medical assessments in order to understand the capacity of the employee/worker/ individual/ for example psych tests for contributors etc.
- Historical purposes for programme making which creates and archives information which is in the public interest.
- Finally where your processing is in the substantial public interest, provided the special category data you use is proportionate and fair with measures that safeguard the rights of the relevant persons.

12. Lawful basis on which a Producer can handle children's data

Children's data needs to be treated with particular care under the GDPR.

You can use any of the lawful bases for processing set out in the GDPR when processing children's personal data. Fairness should be central to all your processing of children's personal data, but for some bases there are additional things you need to think about when your data subject is a young child under 13 such as whether you need parental or guardian's consent.

- **Consent**: If you wish to rely on the child's consent as your lawful basis for processing, then you need to ensure that the child is old enough to understand what they are consenting to, otherwise the consent is not 'informed' and therefore invalid. It is the Controller's responsibility to verify who needs to give consent. There are also some additional rules for online consent, a child under 13 will require parental or legal guardian consent. Please be aware of the implications that can arise when relying on consent as your basis for processing. More information on this is found in point 10.1 as well as on ICO's websites.

- **Contract**: If you wish to rely on 'performance of a contract' as your lawful basis for processing, then you must consider the child's competence to agree to the contract and to understand the implications of this processing and seek parental or guardian's consent if appropriate. It's important to note that under the Ofcom Broadcast Code children are referred to as under 18's.

  For more information on Ofcom's protecting under 18's:
  https://www.ofcom.org.uk/tv-radio-and-on-demand/broadcast-codes/broadcast-code/section-one-protecting-under-eighteens

- **Legitimate Interests:** If you wish to rely upon legitimate interests as your lawful basis for processing you must balance your own (or a third party's) legitimate interests in processing the personal data against the interests and fundamental rights and freedoms of the child. This involves a written asessement and judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to safeguard against those risks.

ICO has further guidance available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

13. Collection of personal data – Privacy Notice

A privacy notice is a statement that tells an individual who is collecting their personal information and what it will be used for and details of any third parties the personal data is going to be shared with as part of the project or making the programme. The GDPR requires a data controller to provide more information about how personal data is to be processed at the point of collection which is often best included in the privacy notice.

Privacy notices take a number of forms, for example a notice on a website or a script read out over the telephone. It should be clear and concise and easily accessible by individuals, and you should document how and when this notice was given. Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

The GDPR says that the information you provide must be:
- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.
- Contain the intended purposes for processing the personal data; and
- The lawful basis for the processing.

A privacy notice should be specific to the project or programme being made. This should differ from a company data protection policy, which is a document that goes into more detail about how your company collects and processes personal data, data subjects' rights and the company's objectives and responsibilities in relation to personal data.

14. What information you need to provide in the privacy notice

- **Who you are:** Details of company, any affiliates/associates linked to you in making the programme/the project.

- **Who is your Data Protection Officer/ Data Manager/ Senior Data Advisor:** (if you have one) or lead or general contact details.

- **What Data You Collect and Process in the programme/project: list,** what personal information you obtain/process; reasons for processing, is there more than one controller?

- **Lawful basis for use of Data:** The lawful basis for processing, what you intend to do with the data and when you will/will not process it.

- **If you are relying on lawful basis of consent.** Display clearly and prominently. Ask individuals to positively opt in and mention the ability and means by which an individual may withdraw their consent. Separate unticked opt in box for direct marketing.

- **Sharing Data:** Who do you share personal data with and why for example if you there is a possibility that you will share psych reports with your broadcaster, you should specify this here. It will be considered good practice to add a link to your privacy policy where whom you are sharing data with should be explained and set out.

- **Legitimate interests**: If legitimate interest is to be relied on as the lawful basis of processing, then you need to set out what legitimate interests apply and take account of the balancing test.

- **Personal data transferred outside the EEA:** if transferring personal data outside the EEA you need to take into account the safeguards that need to be in place.

- **Additional information you will need to take into account:** the retention period; where to go for information about data subjects' rights (ie the privacy policy); the right to lodge a complaint with the ICO; and information about automated decision making.

- **Privacy notices for vulnerable groups:** If you collect information from vulnerable individuals, such as children, you must make sure those individuals are treated fairly. This involves drafting privacy notices appropriate to the level of understanding of your intended audience. **I.e.** age-appropriate language**.** Use child friendly ways of presenting privacy information, such as: diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols, as well as considering the age of the child and whether you also need to provide the individual's parent, guardian or carer with the information.

- **Privacy notices for people whose first language is not English:** if you are collecting information from people whose first language is not English, you may need to consider if you should provide your privacy notices in another language although you are not be required by law to offer translations.

- **Children's consent for online service**: Parental permission is required to process the personal data of children (a child is anyone under the age of 16 for GDPR). In some contexts (especially online), proving parental or legal guardian permission has been obtained may be difficult. If you are relying on consent as your lawful basis for processing personal data when offering an online service directly to a child, only children aged 13 or over are able provide their own consent in the UK under the DPA 2018; under 13's will require parental or legal guardian consent. If targeting wider European markets, ensure you comply with the age limits applicable in each Member State, eg in France and Germany the age of online consent is 16 (the applicable age limit will be set out in that Member States legislation which implements GDPR).

Please see related ICO guidance:

Legitimate interest: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/

Transfers outside the EEA: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

Accountability & Governance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

Right to be informed: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Automated profiling: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

15. Rights of individuals and what to consider when drafting your privacy policy.

The GDPR establishes 8 specific rights for the data subject, and you need to show compliance by incorporating these rights into how you process data. Children have the same rights as adults over their personal data. Further details on individual rights in the GDPR are are explained below.

15.1 Right to be informed:

Individuals have the right to be informed about the use of their personal data and should be given the information at the time you collect the personal data from them. If you obtain personal data from other sources, you must provide individuals with privacy information at the first communication with the data subject, or when personal data are first disclosed to another recipient. However, this must be **no later than one month** after having obtained the data.

Children have the same rights as adults over their personal data and can exercise their own rights as long as they are competent to do so. It is good practice to also explain the risks inherent in the processing and the safeguards you have put in place. Where a child is not considered to be competent, an adult with parental responsibility may exercise the child's data protection rights on their behalf. If you are relying upon parental consent as your lawful basis for processing it is good practice to provide separate privacy notices aimed at both the child and the responsible adult.

Please read the ICO guidance on right to be informed:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

15.2 Right of Access - known as a Subject Access Request ('SAR')

Under the GDPR, individuals have the right to request a copy of all information which is held about them by you (i.e. their personal data). This may be held on a computer and/or and in certain paper records.

The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request to you verbally or in writing. Before providing copies of the information you must satisfy yourself as to the identity of the person seeking the information, and that they are authorised to receive it. You can ask for more information to help you confirm their identity. You are entitled to seek proof of identity, for example a copy of photo identification or proof of address.

In the event you receive a subject access request you must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive, or if copies of the same information are required. You should seek to respond to a request as soon as possible but no later than one month from receipt of request.

There are a number of exemptions to providing information in response to a subject access request. For example, legal professional privilege, negotiations with the data subject if likely to prejudice such negotiations, management forecasting or planning if disclosure would prejudice the conduct of the business, and confidential references. It's important to be aware that exemptions are not to be used as a default position, and each application of an exemption needs to be justified.

In particular, you should remember that you **may** be exempt from providing data associated with programme-making (including rushes) under 'the special purposes exemption' i.e processing for journalisitcm academic, literary or artistic purposes set out in Schedule 2, Part 5 Section 26 DPA 2018.

If you decide not to provide the individual with a copy of their data, you should explain your decision and inform them of their right to make a complaint to the ICO and their ability to seek to enforce their rights through a judicial remedy.

Please read the right of access to information on the ICO website:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Further guidance on the exemptions and how to apply them is available from the Information Commissioner.

A new code of practice on dealing with subject access requests is also available from their website:
http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF

Producers Note:

Where the request relates to programme material including rushes, you should consult with your commissioning broadcaster to discuss any legitimate legal and editorial grounds there might be for resisiting or if any further actions are necessary before making a disclosure (i.e deleting in case it infringes someone else's rights).

15.3 Right to Rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request for rectification verbally or in writing.

You can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, or the request is repetitive in nature. You can request a 'reasonable fee' to deal with the request. If you have doubts about the identity of the person making the request, you can ask for more information.

If you consider the information is correct: You should let the individual know if you are satisfied that the personal data is accurate and tell them that you will not be amending the data.

If you rectify the data and have already disclosed the personal data to others, you must contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individual about these recipients.

You have **one calendar month** to respond to a request. You should explain your decision and inform them of their right to make a complaint and their ability to seek to enforce their rights through a judicial remedy.

ICO guidance on right to retification can be found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

Producer Note:

Where the request relates to programme material you may wish to consult with your commissioning broadcaster before making any disclosure regarding rectification as there may be legitimate legal and editorial grounds for resisting changes to the information.

15.4 Right of Erasure, the Right to be Forgotten

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. The right is not absolute and only applies in certain circumstances. You **have one month** to respond to a request. If you have doubts about the identity of the person making the request, you can request more information from them.

Individuals have the right to have their personal data erased if;

- The personal data is no longer necessary for the purpose for which it was originally collected or if you are relying on consent as your lawful basis for holding the data, and the individual withdraws consent;

- You are relying on legitimate interests or the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- If you have processed the data unlawfully (in breach of the 1st Data protection principle);
- If you are processing the personal data for direct marketing purposes and the individual objects;
- If it is to comply with a legal obligation; or you have processed the personal data to offer information society services to a child.

Children's information:

- There is an emphasis on the right to have personal data erased if the request relates to data collected from children. If you process data collected from children, you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child because a child may not have been fully aware of the risks involved in the processing at the time of consent.

When does the right to erasure/the right to be forgotten not apply?
The right does not not apply if the processing is necessary for one of the following reasons:
- To exercise the right of freedom of expression and information;
- To comply with a legal obligation;
- For the performance of a task carried out in the public interest or in the exercise of official authority;
- For archiving purposes in the public interest, scientific research, historical research, or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing;
- For the establishment, exercise or defence of legal claims.

Please read ICO guidance on right to erasure:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

15.5 Right to Restriction

Individuals have the right to restrict or suppress their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restriced, you are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. You have **one calender month** to respond to a request.

The GDPR suggests a number of different methods that could be used to restrict data, such as:
- Temporarily moving the data to another processing system;
- Making the data unavailable to users; or
- Temporarily removing published data from a website.

You can refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

ICO guidance on right to restrict processing:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

15.6 Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. You must act upfront the request without undue delay and at the latest within **one calendar month** of receipt.

The right to data portability only applies:
- to personal data an individual has provided to a data controller;
- where the processing is based on the individual's consent or for the performance of a contract;
- and when processing is also being carried out by automated means.

You can refuse to comply with a request for data portability if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

Please read ICO guidance on data portability:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

15.7 Right to Object

The GDPR gives individiduals the right to object to the processing of their personal data in certain circumstances. An individual can make an objection verbally or in writing. You have **one calendar month** to respond to an objection. Individuals have the right to object to processing of their data if it is being handled on a legitimate interests basis or if for the performance of a task carried out in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

If you process data for the performance of a legal task or for your organisation's legitimate purpose or direct marketing, you must inform individuals of their right to object "at the point of first communication" and in your privacy notice. When an individual objects, they must have an objection on "grounds relating to his or her particular situation".

If you process personal data for research purposes, individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object. If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

You do not need to stop processing - if you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or the processing is for the establishment, exercise, or defence of legal claims.

Children's information - children have the same right as adults to object to you processing their personal data for direct marketing, so, you must stop doing this if a child (or someone acting on their behalf) asks you to, children merit specific protection when you are using their personal data for marketing purposes.

ICO guidance on the right to object:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

15.8 Rights related to automated decision making including profiling

The GDPR applies to all automated individual decision-making. It's this right that applies to decision making that has a legal or similarly significant effects on individuals whose data is being processed. his relates to where there is a decision solely made by automated means without any human involvement and profiling (automated processing of personal data to evaluate certain things about an individual).

Article 22 in the GDPR essentially acts as a prohibition against this type of decision making unless one of the conditions apply. Therefore you can carry out this type of decision-making only where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by union or member state law applicable to the controller; or
- based on the individual's explicit consent.

You must identify whether any of your processing falls under this provision and, if so, make sure that you:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

Children's information: You should not make decisions about children that are based solely on automated processing, (including profiling), if these have a legal effect on the child, or similarly significantly affect them. If you profile children, then you must provide them with clear information about what you are doing with their personal data. You should not exploit any lack of understanding or vulnerability.

You should generally avoid profiling children for marketing purposes. You must respect a child's absolute right to object to profiling that is related to direct marketing and stop doing this if they ask you to. It is possible for behavioural advertising to 'similarly significantly affect' a child. It depends on the nature of the choices and behaviour it seeks to influence.

More information on the application to children is available on the ICO website:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/

ICO guidance on on rights related to aumotated decision making:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

16. Exemptions

16.1 Journalisitic, academic, artistic and literary

This exemption is based on the GDPR article 85(2) for reasons of freedom of expression and information and can be found in Schedule 2 Part 5 paragraph 26 of the DPA 2018. The exemption criteria appears to be substantively the same as to the DPA 1998. Article 85(2) GDPR requires a balancing of fundamental rights under the EU Charter of Fundamental Rights. Article 11 of of the charter is the freedom of expression, while Article 7 and Article 8 provide for rights to privacy and data protection.

Its important to note that under DPA 2018 there is not a blanket exemption from data protection and shouldn't be used in a blanket manner. Even when this exemption applies, it only exempts it from specific provisions, and only insofar as these are incompatible with the special purpose.

16.1.1 Special purpose

Under the DPA 2018 Act 'special purposes' means for the purposes of journalism, academic (academic is a new provision), artistic and literary purposes. These special purposes are exempted from certain conditions under GDPR,provided that;

- the data in question must be being processed with a view to the publication of journalistic, academic, artistic and/or literarymaterial,
- the data controller must *reasonably believe* that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and
- the data controller must *reasonably believe* that the application of the listed GDPR provision would be incompatible with its journalistic, academic, artistic and/or literary purpose.
- Assuming these criteria are met, a data controller will be exempt from complying with the GDPR rights and obligations in relation to processing of personal data eg, making a programme. The specifics of what it does exempt from are listed in Sch 2, 26(9) DPA. Following the accountability principle in the GDPR, it is important that you are able to document and record your decision on the application of the exemption.

16.1.2 Security measures

Its important to note that there is no exemption under DPA 2018[1] in respect of the principle that personal data must be processed with appropriate technical and organisational measures to ensure it is processed fairly and lawfully.[2]

[1] in respect of the obligation under Article 5(f) of the GDPR
[2] see s.32(2)(a) DPA 1998 and Paragraph 26(9)(i) DPA 2018).

16.1.3 Codes of practice

The codes of practice have added importance for a publisher seeking to rely on the exemption. The DPA 2018[3] provides explicitly that when forming a belief that publication is in the public interest a data controller *must* have regard to relevant codes of practice, namely the BBC Editorial Guidelines, the Ofcom Broadcasting Code and the Editors' Code of Practice. The Secretary of State can also add extra codes of practice.[4]

16.1.4 Statutory stay

The "stay" mechanism to prevent data protection being used to obtain a pre-publication injunction (in respect of material not published, or published for less than 24 hours) is retained in s.176. However section 174(3)(b) of the DPA 2018 provides that the ICO may determine whether personal data are either not being processed only for the special purposes; or whether the data are being processed without a view to the publication of journalistic material that has not previously been published.

16.1.5 Criminal data offences

New criminal data offences have been introduced alongside explicit journalism public interest defences at ss170-171 of the DPA 2018. This adds to the existing offence of unlawfully obtaining personal data, a new offence of re-identification of de-identified personal data. Given the risk of impinging on investigative journalism, each offence provides expressly for new defences that mirror the special purposes exemption.

16.1.6 Guidance, review and reporting obligations

The ICO has had its responsibilities as a watchdogs over the media increased as follows:

- In relation to the media industry it is to produce guidance on how to seek redress against media organisations where an individual considers that a media organisation has failed to comply with data protection legislation. This will not necessarily apply to online platforms. [5]
- The ICO is to consult prepare and submit to the Secretary of State a code of practice to be approved by Parliament containing practical guidance on compliant processing of personal data for the purposes of journalism and practice which is desirable having regard to the interests of data subjects and the special importance of the public interest in freedom of expression and information .
- The ICO is to carry out periodic reviews of whether the data protection legislation is being complied with by the media and report their findings to the Secretary of State..[6]
- Separately the Secretary of State must report to Parliament on the use and effectiveness of the media's dispute resolution procedures in cases involving allegations of breaches of data protection legislation, specifically on any dispute resolution procedures provided by those who enforce codes of practice for relevant media organisations.[7] This will include IPSO, IMPRESS and, perhaps unintentionally since what constitutes an alternative dispute resolution procedure is not defined, potentially also OFCOM in so far as its code relates to on-demand publishers.

The ICO are updating their guidance for the media industry in the mean time you should speak with your commissioning broadcaster or consult a lawyer when the Exemptions under Schedule 2 Part 5, section 26 of the DPA 2018.

17. Accountability and Governance

Accountability is a new requirement under GDPR – you are responsible for complying with the GDPR **and** now you must be able to demonstrate your compliance. Putting in place relevant policies demonstrates your approach to compliance.

You need to put in place appropriate technical and organisational measures to meet the requirements of accountability. Organisations that adopt a best practice approach to compliance with the DPA 1998 Act should be well placed to adapt to the new requirements. However, you should review them for the GDPR.

[3] Paragraph 26(5)
[4] Paragraph 26(7)
[5] s.177 DPA 2018;
[6] s.178 DPA 2018 and Schedule 17.
[7] s.179 DPA 2018.

The following are considered relevant in demonstrating accountability:

- Adopting and implementing data protection policies;
- Documenting your processing activities; recording and reporting personal data breaches;
- Creating, implementing, and improving appropriate security measures;
- Putting written contracts in place with organisations that process personal data on your behalf;
- Taking a 'data protection by design and default' approach such as privacy impact assessments and privacy by design which includes measures such as minimising the data you collect, applying pseudonymisation techniques, and improving security features;
- Use **data protection impact assessments (DPIA)** for uses of personal data that are likely to result in high risk to individuals' interests;
- Adhering to approved **codes of conduct and/or certification** schemes;
- Appointing a data protection officer (where necessary); and
- Ensuring a good level of understanding and awareness of data protection amongst your staff;

17.1 Data Protection Impact Assessments

Data Protection Impact Assessments ('**DPIA**') are now legally required if the processing is **likely to result in a high risk** to individuals' interests. To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. A DPIA is a process to help you identify and minimise the data protection risks of a project. You should speak with your commissioning broadcaster if you consider a DPIA necessary and require their input.

ICO has published a list of practical examples of the types of processing operations which would require DPIA as set out under the GDPR. It is intended to help controllers understand when a DPIA is automatically required or considered good practice.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

What should form part of the DPIA is set out here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

ICO also has provided a suggested template of a DPIA:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

17.2 Data protection by design and default

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you integrated data protection into your processing activities.

The ICO is working to update this guidance to reflect the provisions of the GDPR. In the meantime, the existing guidance is a good starting point for organisations, see the ICO website:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

17.3 Anonymisation of data

The GDPR does not apply to anonymised information. Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. Effective anonymisation can be used to publish data which would otherwise be personal data.

The ICO defines anonymisation as: the process of rendering data into a form which does not identify individuals and where identification is not likely to take place through its combination with other data. Once data is truly anonymised and individuals are no longer identifiable, the data will not fall within the scope of the GDPR and it becomes easier to use.

To identify whether effective Anonymisation can be achieved, it is sensible to conduct a thorough Risk Assessment of whether any organisation or member of the public could identify any individual from the data being released – either in itself or in combination with other available information.

A useful test is the **Motivated Intruder Test** which involves considering whether an 'intruder' would be able to achieve re-identification *if* motivated to attempt this. The 'motivated intruder' is taken to be a person who starts without any prior knowledge but who wishes to identify the individual from whose personal data the anonymised data has been derived. As an overview the 'motivated intruder' is reasonably competent, but is not assumed to have any specialist knowledge.

A trusted third party (TTP) arrangement can be particularly effective where a number of organisations each want to anonymise the personal data they hold for use in a collaborative project. Typically, the TTP will operate a data repository to which the various participating organisations will disclose their personal data.

Anonymisation might be used where audience members wish to share their stories or experiences, but the data provided is sensitive. For example, if individuals wanted to contribute to a story about their experiences with the NHS, those contributions might need to be aggregated or anonymised in order to provide support for a story without linking it to a specific individual. Anonymisation might also be used where an organisation wishes to share data for research purposes.

See ICO: http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation

18. Security of personal data ('Security Principle')

A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures.' This replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the DPA 1998.

This means that you need to have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. The security principle goes beyond the way you store or transmit. This means every aspect of your processing of personal data is covered, not just cybersecurity.

What is 'appropriate' for you will depend on your company's circumstances. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive, or confidential it is – as well as the damage or distress that may be caused if the data was compromised. The ICO will consider the technical and organisational measures you had in place when considering an administrative fine.

Under the DPA 1998, the ICO published a number of detailed guidance pieces on different aspects of IT security. The ICO will be updating their guidance to reflect the GDPR's requirements in due course.

19. Recommended practices for security of personal data

A production company should regularly review how it stores all personal data, including for those individuals whose personal data is collected during the course of making the programme, to assess whether the security measures in place can be improved. As well as restrict those authorised who can access, alter, disclose or delete.

If personal data is accidentally lost, altered or destroyed, you should be able to recover it, and therefore prevent any damage or distress to the individuals.

The less personal data which you have, the more you lessen your risk. As such, if you have appropriate retention schedules in place which are followed, you lower the risk of data loss. However, there is always a need for some personal data to be held and this should be appropriately secured. Some suggestions for doing so are set out below.

19.1 On premises security

- Can hard copies of production and other files be kept in locked cabinets and/or is there secure storage on or off the site?

- Do office computers and networks have sufficient information security measures in place? Are passwords restricted and regularly updated?

- Is access to computer files with personal data limited to those who actually require access, and are computers logged off overnight or locked if left unattended?

- Do computer systems have adequate virus protections and firewalls etc., and is guidance given to staff about the necessary care to be taken when opening emails and attachments or visiting new websites?

- Are adequate measures in place for back-ups of personal data, to prevent accidental destruction?

- Are computer screens/notice boards and white boards positioned away from windows/public view to prevent accidental disclosures of personal data? Are appropriate measures taken so that paper documents cannot be viewed by unauthorised visitors?

- Is access to the building controlled and are adequate and reasonable security measures in place? Are visitors adequately supervised or monitored near personal and other confidential information?

Where CCTV is in operation is this in compliance with the CCTV code of practice provided by the Information Commissioners Office?

Please note that this ICO guidance is still to be updated to comply with the GDPR – but is a good place to start: http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

For additional guidance on IT security for the GDPR please refer to:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

19.2 Off premises security

- Are computers, laptops, computer discs, memory sticks, etc. allowed off the premises and, if so, is there suitable password protection in place for personal data, special category data, criminal data, children's data, financial data (or other data such as major talent contact details)? Is there a high level of encryption for the relevant folder or for the computer/discs etc. as a whole, or other protection arranged? If the equipment was stolen would the personal data be protected?

- Have you considered ICO's guidance on implementing encryption: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/implementing-encryption/ Are encryption products certified to meet the current GDPR standards?

- Has the ICO guidance that all portable media devices containing personal data should be encrypted to FIPS 140-2 (cryptographic modules, software and hardware) and FIPS – 197 (or as otherwise suggested by the ICO from time to time) been properly adopted? The guidance is available at: http://ico.org.uk/news/current_topics/Our_approach_to_encryption Please note that this guidance has not been updated with additional GDPR information.

- Are work mobile devices password locked and/or coded?

- Where accessing broadband and a link is available, are suitable protections in place for accessing the information, i.e password protected/secure network?

- Is suitable guidance given on the protection, return and/or destruction of documents, memory sticks, and/or DVDs that need to be taken off the premises? Do you have mechanisms in place for ensuring staff are aware of and follow this guidance? Have you distributed the Crew Data Security Guidelines? Do you provide opportunities to staff on understanding their GDPR obligations? Do staff/crew know who to contact in the event of a data breach?

- Is there a system in place for tracking information where data is taken off site and returned?

- Are adequate provisions for secure storage of production paperwork, call sheets, release forms, made available when off site to ensure documentation is not left lying around?

- Is any personal data, special category, children data being stored in a cloud based storage system or collaboration tool? If so, are there adequate protections in place to ensure the security of data using such storage?

- If you use any online services or suppliers (for example Mailchimp for sending out newsletters or Dropbox to send files) it is your responsibility to check that they are GDPR compliant. Ways to check if they are compliant is to go to their website and read their privacy policy and terms of use or check that their terms include appropriate processor wording, or you can email them to ask. If the services and suppliers are not GDPR compliant, you should consider looking for alternative services that are GDPR compliant. This because the ultimate responsibility rests with the company.

19.3 Information collection and disposal

- Is unnecessary copying of paper and electronic records for distribution being undertaken? Are staff aware that they should be careful not to leave copies of documents at the photocopier, scanner, or fax machine?

- Are shredders and/or "security safe" recycling bins/boxes readily available for disposing of documents and papers potentially containing personal data, and are staff reminded to use them properly?

- Is the requisite care and attention taken when faxing personal data so that only the intended recipient receives the information at the time of sending the information? The ICO recommends reducing the number of faxes you send as faxing has been the subject of many civil monetary penalties. If sending a fax is essential, confirming receipt of personal data sent via fax is recommended.

- Are employees and workers aware that even verbal disclosure of personal data can be in breach of GDPR and are they aware of when it is appropriate to disclose?

- Where you receive a request for information from the police you are not compelled to provide the information. However, you may choose to provide the information if a senior member of your company is satisfied that you have complied with the following guidelines (this is still to be updated with GDPR):

  http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/SECTION_29_GPN_V1.ashx.

  Where an application for information is related to programme material or rushes you should consult with your commissioning broadcaster before any disclosure takes place as there may be legitimate legal and editorial grounds for resisting disclosure.

- On close down of a production senior staff should review what personal data records can be legitimately retained or destroyed.

- If you are selling or disposing of computers, disks, or memory sticks, have you taken appropriate steps to ensure that any personal data stored on such devices have been securely deleted or made unavailable to future users?

- Consideration should be given to the legitimacy of keeping records. For example, records of quiz show applicants who are not in the final programme should be destroyed unless they have given permission for the records to be kept for future series or other shows or there is another legitimate business or legal reason to retain them, (e.g. they had an accident at the audition and it is required for health and safety reasons), but the records of an actor who does not make the final cut may still need to be held for a limited time for e.g. auditing purposes.

- When staff leave your employment are they reminded or obliged to **leave behind and /or delete** all confidential and/or appropriate personal data?

20. Can I use the personal data for our other projects or for marketing?

You must only use personal data for the limited purposes for which it was collected or given to you. For example, it may be that the personal data was only provided by a contributor for the purposes of a particular programme and not

for any other use. This means that you must not sell, distribute, or provide this personal data in any other form to any third party, except where this is necessary to produce and exploit the Programme.

However, if you obtain express consent from the person to contact them in the future to be involved in other programmes, or to receive marketing information, or to contact employees for opportunities for work etc then you are permitted to do so (these consents should be regulary reviewed). Where you want to provide individuals with electronic marketing messages (e.g. SMS or email marketing), their express consent is required (except in limited circumstances). This can be agreed for example when a contributor signs the form or when contracting with an employee or worker, the lawful basis on which you use the data must be clear.

21. Use of online tracking tools such as cookies.

21.1 Cookies

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') deals with the use of cookies and other information which can be stored on an individual's device. A cookie is a small amount of data, which often includes a unique identifier that is sent to your computer or mobile phone (referred to here as a "device") browser from a website's computer and is stored on your device's hard drive. Any company using cookies or similar technology is required to ensure that they are taking necessary steps to comply with the Regulations.

Cookies or similar devices must not be used unless the subscriber or user of the relevant terminal equipment:

- Provides with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
- Has given his or her consent.

Advice on the use of cookies can be found on the ICO website in the guidance entitled:
"Guidance on the use of cookies and similar technologies"
http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies

The Privacy and Electronic Communications (EC Directive) Regulations 2003 are due to be updated in 2019 It is intended to provide individuals with clearer information and more control over the use of cookies when visiting websites and services as well as'prevent pop ups' where users are bombarded with approvals to land cookies. More to come on these new changes.

21.2 Location Data

In some circumstances, organisations who offer services related to smartphones or GPS may be processing location data (for example postcodes map references or any other data revealing the geographic position of a user's mobile device). PECR lays down very specific rules for the collection and use of location data and requires 'consent' whenever collecting data about mobile users' locations. Publishers must not collect geolocation information about their users unless and until this consent has been sought.

Location data might be used in a number of ways. For example, by companies who produce digital content, such as apps or for example personalisation e.g. in weather apps to provide detailed information on local weather, or in UGC e.g. where audience members are invited to take photos, tag their location, and upload the photos to a programme's website.

Please read the ICO guidance on Location Data:
https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/

22. Do I need a Data Protection Officer?

The GDPR introduces an obligation appoint a Data Protection Officer ('**DPO**') if your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or of large scale processing of special categories of data or data relating to criminal convictions and offences.

You can appoint a DPO if you wish, even if you are not required to. If you decide to voluntarily appoint a DPO you should be aware that the same requirements of the position and tasks apply had the appointment of a DPO been mandatory.

In any event, irrespective of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and resources to discharge your obligations under the GDPR. If you do not need to appoint a DPO, either voluntarily or because you do not meet the above criteria, it is adviseable to record this decision to help demonstrate compliance with the accountability principle. It's important that if you are not appointing a statutory DPO to not call the responsible person a DPO unless that is to be their role, a more appropriate title would be for example a Data Manager.

- If appointing a DPO, this person will be the first point of contact for ICO and for individuals whose data you process. You will need to publish your DPO details and provide them to the ICO.

- A DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. A DPO can be an existing employee or externally appointed (as long as their role does not create / or is in conflict). In some cases, several organisations can appoint a single DPO between them.

- A DPO should monitor compliance with the GDPR your data protection polices, internal data protection activities; raise awareness of data protection issues, train staff, conduct internal audits advise on and monitor data protection impact assessments ;

- You must provide adequate resources (sufficient time, financial resource, infrastructure, and, where appropriate, staff) to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge.

The ICO guidance on Data Protection Officers can be found here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

23. What if you become aware of a breach, loss of security or an unauthorised disclosure?

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. This includes breaches that are the result of both accidental and deliberate causes, alteration of data without permission. It also means that a breach is more than just about losing personal data.

If you become aware of a breach of the GDPR, you should alert your line manager, DPO or the senior member of your staff responsible for GDPR matters immediately, because prompt action is required.

You should also take immediate action to identify the potential harm to the person(s) concerned.

If the breach relates to programme material e.g. it relates to contributors, contestants or talent you should also alert your commissioning broadcaster as soon as possible and take any further action that may be advisable.

23.1 What breaches do we need to notify the ICO about?

Under the GDPR, when a personal data breach has occurred, the controller shall without undue delay notify the supervisory authority (the ICO in the UK) **unless** the breach is unlikely to result in a risk to the rights and freedoms of individuals. Therefore you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a high risk, then the ICO must be notified; if it is unlikely that there will be a risk to a person's rights or freedoms, then you do not have to report it to the ICO. However, if you decide you do not need to report the breach, you need to be able to justify this decision. So, the breach and your decision in regards to reporting, must be documented. You need to assess this on a case by case basis, looking at all relevant factors. You may also need to notify the data subjects concerned without undue delay if there is a high risk to the rights and freedoms of individuals and harm is likely to be suffered by individuals.

If the breach relates to programme material you should also alert your commissioning broadcaster as soon as possible and take any further action that may be advisable. It may be appropriate in some instances that you may decide with your commissioner that the broadcasters is best to notify the ICO if they are the data controller. A processor should notify a data controller without undue delay after becoming aware of a data breach.

If the breach is one that needs to be reported, you must notify ICO (if a high risk) no later than 72 hours after becoming aware of it. If you take longer than this, you must give suitable reasons for the delay. In the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority.

ICO provide additional guidance on reporting to ICO: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

23.2 What are the penalties for unauthorised disclosure?

The Information Commissioner's Office ('the ICO') investigates all breaches of the GDPR. The ICO can impose sanctions (including criminal sanctions) against companies found to be in breach. The ICO has the power to fine organisations up to 10 million Euros or 2 percent of your global turnover for breach of the GDPR including for failing to report a breach to the regulator within 72 hours, with also further sanctions. Fines of up to 20 million Euros or 4 per cent of your global turnover can be imposed for serious breaches including breach of the security leading to significant harm to individuals.

24. Reputational damage

In addition to the statutory sanctions that the ICO can impose on a company, there is a significant risk of reputational damage to the company or broadcaster if a breach occurs. This can be compounded where talent is involved. Press criticism directed at a production company, talent and broadcaster can be highly damaging. In addition, contributors are less likely to want to disclose personal data to a production company if they believe that their personal data will not be kept securely.

25. Additional guidance and information

For additional guidance and information, please refer to the Information Commissioner's Office at www.ico.org.uk.

- For more information on the Data Protection Act 2018 please visit: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- GDPR Regulations: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

END