Producers' Data Protection and Security Guidelines

1. Introduction

These guidelines set out recommended safeguards that all production companies should implement in order to best protect all **Personal Data** (including **Sensitive Personal Data)** and to ensure compliance with the Data Protection Act 1998 ('**DPA**'). A copy of the DPA together with practice guidance notes can be found on the Information Commissioner's website at: - http://www.ico.org.uk/. 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 (including Sensitive Personal Data) under the DPA.

The guidelines are designed to provide practical advice to assist in protecting the data of individuals and in turn protecting production companies from civil and/or criminal sanctions and reputational damage as the result of an unauthorised disclosure of Personal or Sensitive Personal Data under the DPA.

It is therefore important that all senior staff read these guidelines and that the necessary practical support and guidance is provided for all staff. It is recommended that one senior person within the company takes overall responsibility for data protection policy and practice for the company. Contact details of that senior person should be made available and accessible to all staff.

2. What is Personal Data?

Personal Data is data which relates to a **living individual** who can be identified from that data, or from that data in conjunction with other readily available information, e.g. **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. It can also include data such as IP addresses and data automatically collected when using computers and the internet.

3. What is Sensitive Personal Data?

Sensitive Personal Data is data that relates to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health matters, sexual orientation/life, alleged or actual criminal activity and criminal records. The processing of Sensitive Personal Data requires extra care and, except in limited circumstances, Sensitive Personal Data can usually only be collected and used **with the express consent** of the person to whom the data relates.

4. Notification to the Information Commissioner

If you make decisions about how Personal Data is processed and collected it is likely that your company will need to notify the Information Commissioner for listing on the Information Commissioner's register. This is a legal requirement and failure to keep registered details up to date is a criminal offence. If you are processing Personal Data it can be safely assumed that this is something that you do need to do (if you haven't already done so).

Please refer to http://ico.org.uk/for_organisations/data_protection/registration

5. Collection of and access to Personal Data

You and the employees and freelancers working for you 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 might be contained or provided in letters, correspondence, call logs, programme treatments, running orders, CVs, CCTV footage, contributor agreements or release forms, contributor application forms, call sheets, P-as-Cs, criminal record bureau and/or disclosure & barring service checks, medical records, invoices, purchase orders, rushes with captions, bank statements, lists of employees, and employee references. The 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 Data collected to what is actually and likely to be needed. For example, it is unlikely that you would need information regarding a contributor's sexual history, unless it was relevant to the programme.

When you are collecting Personal Data from individuals, you should tell the individual why you are doing so, who you are and any additional information necessary if specific circumstances require it. The ICO guidance provides that you do not need to tell people what you are doing if the use is obvious, i.e. when having a release form signed with a description of the programmes, it is obvious to the reasonable person, why and how the information will be used, in such circumstances a written privacy notice is not necessary. A privacy notice is a statement that tells an individual who is collecting information and what it will be used for and details of any third parties the Personal Data is going to be shared with. Privacy notices take a number of forms, for example a notice on a website or a script read out over the telephone.

Where you are collecting confidential and/or Sensitive Personal Data, or are intending to use Personal Data in a way that is likely to be unexpected or objectionable to the individual, you must actively communicate your privacy notice i.e. take positive action to provide the privacy notice to the individual, for example, the policy could form part of the contract with the individual. Please read the ICO's codes of practice relating to **Privacy Notices and the Personal Information Online: code of practice**. Links to these two documents (amongst other ICO guidance) can be found at:

http://ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications

The ICO has launched guidance on privacy impact assessments (PIAs) a tool that can be employed to help assess and minimise the risk of misusing data. Pact is in the process of developing a pan industry approach to PIAs. Further information on PIAs are available at:

http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf

6. Policies & Personnel

All production companies must have in place an appropriate Data Protection or equivalent Security Policy that sets out how they manage Personal Data within the company and when making programmes. The policy should incorporate the **eight principles** contained in the DPA. This means that all companies must take prudent steps to ensure Personal Data is:-

1) processed fairly and lawfully;

2) processed for specified and lawful purposes;

3) kept to a minimum when it is collected and processed. That is only Personal Data which is adequate, relevant and not excessive is processed ;

4) accurate and, where necessary, kept up-to-date;

5) not kept longer than is necessary;

6) processed in accordance with the rights of the data subjects under the DPA;

7) Secured using appropriate technical and organisational measures to protect against unlawful or unauthorised processing of Personal Data and against accidental loss, destruction or damage to Personal Data;

8) not transferred outside the European Economic Area unless that country has an adequate level of protection in respect of the processing of Personal Data.

Steps should be taken to alert and advise employees and workers of their obligations under the DPA and of your data protection and security policies and practices. The ICO website provides useful information to help with most compliance issues. If there are specific detailed enquiries then the ICO telephone helpline can help answer these. You may also want to consider if it would be helpful for any individuals to attend a training session or course in order for them to help them understand your obligations under the DPA. There are a number of organisations who can provide suitable training courses.

7. Exemptions

There are some limited exemptions under the DPA where the processing of Personal Data will be exempt from a number of the eight data protection principles (see paragraph 6 above). However, no exemption exists surrounding data security so it's important that Personal Data is always protected against unlawful or unauthorised processing and against accidental loss, destruction or damage.

In certain circumstances where you are processing Personal Data with a view to publishing journalistic, literary or artistic material ('the special purposes exemption' under section 32 DPA) you **may** be exempt from certain provisions of the DPA provided that the personal data are processed only for these special purposes, there is a reasonable belief that such publication would be in the public interest and there is a reasonable belief that in all the circumstances compliance with certain provisions of the DPA would be incompatible with the special purposes. Further requirements apply to the processing of Sensitive Personal Data.

Further guidance on the exemptions and how to apply them is available from the Information Commissioner or alternatively you should consult a lawyer.

[See also paragraph 17 below which deals with Subject Access Requests under the DPA]

8. Recommended practices for security of Personal data

The 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. 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.

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 unused?

- 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? - http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

For additional guidance on IT security please refer to:
http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/it_security_practical_guide.pdf

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, Sensitive Personal Data and financial data (or other data such as children's and 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? Are encryption products certified via CESG's CPA or CAPS schemes to at least Foundation grade to meet the current 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

- 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?

- 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 or Sensitive Personal 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?

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 the DPA 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:

  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 closedown 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 doesn't 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?

9. What if I am engaging a third party to handle Personal Data for the Programme?

If you are using a third party or a sub contractor who is a Data Processor to handle, process or dispose of Personal Data or confidential information on your behalf you must ensure that they undertake to abide by the DPA. You will be responsible for any breaches of the DPA which arise from the activities of the Data Processor. The DPA requires you to have a written contract in place setting out as a minimum that the Data Processor can only act on instructions from you (as Data Controller) and that they have to ensure appropriate security measures are taken against loss, damage to or unauthorised processing of Personal Data. Where a Data Processor is processing Personal Data that, if lost, may cause harm for a production, it will generally be appropriate to (i) expressly provide in your contact with them that they must comply with these guidelines (as applicable) and (ii) include provision in the contract for you to be able to inspect and/or monitor their compliance where practical and necessary.

10. What if I am sharing Personal Data with other organisations?

Data sharing, according to guidance issued by the Information Commissioner's Office includes both the systematic and/or routine sharing of information between and/or within organisations (eg pooling data) as well as the exceptional, one-off decisions to share data (eg requests from the police). When sharing data, you should ensure that you can demonstrate that the appropriate measures have been taken to protect and appropriately use Personal Data. The first step is to establish that the purpose for the sharing of Personal Data is a valid one and that it is actually necessary to share Personal Data in order to achieve that purpose. In doing so, it is recommended that you have regard to the Information Commissioner's Data Sharing Code of Practice.

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

It should be noted that while, for the most part, the Data Sharing Code of Practice is concerned with data sharing between Data Controllers, it also makes reference to sharing within organisations. This is particularly the case where the different areas of an organisation may have a different approach to data protection given the different functions and cultures of the areas of that organisation (eg marketing department as opposed to HR department). The Data Sharing Code of Practice also mentions data sharing between Data Controller and Data Processor. Considerations about such data sharing should be covered off in contract: for more information on this refer to the guidance in paragraph 9 above.

11. 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 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. 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 when the contributor signs the form or when contracting with an employee or worker.

The ICO guidance on electronic marketing can be found at:
http://ico.org.uk/for_organisations/privacy_and_electronic_communications/~/media/documents/library/Privacy_and_electronic/Practical_application/the-guide-to-privacy-and-electronic-communications.pdf

12. Use of online tracking tools such as cookies.

Cookies

The Privacy and Electronic Communications (EC Directive) Regulations 2003 were amended in 2011 to include further requirements in relation to 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.

According to the Regulations, cookies or similar devices must not be used unless the subscriber or user of the relevant terminal equipment:

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) has given his or her consent.

The updated guidance on cookies provides additional information around the issue of implied consent which can be a valid form of consent provided that certain requirements are met.

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" which can be found at:
http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies

Any company using cookies or similar technology is required to ensure that they are taking necessary steps to comply with the Regulations.

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).

Section 14 of The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) lays down very specific rules for the collection and use of location data. In particular, the PECR mandates a requirement for '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, perhaps 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.

13. Anonymisation of data

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.

Factors to take into account include:
- the likelihood of re-identification being attempted;
- the likelihood the re-identification would be successful;
- the anonymisation techniques which are available to use;
- the quality of the data after anonymisation has taken place; and
- whether this will meet the needs of the organisation using the anonymised information.

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.

Governance
Organisations anonymising personal data need an effective and comprehensive governance structure including senior-level oversight of the governance arrangements. The ICO will ask about this if a complaint is received or if it carries out an audit.

Trusted third parties
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.

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

14. What if you become aware of a loss of security or an unauthorised disclosure?

If you become aware of a breach of these guidelines, you should alert your line manager and the senior member of your staff responsible for DP matters immediately, because prompt action is required.

You should also take immediate action to identify the potential harm to the person(s) concerned.
Please read the ICO guidance at: - http://ico.org.uk/for_organisations/data_protection/lose, and take action accordingly.

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

15. What are the penalties for unauthorised disclosure?

The Information Commissioner's Office ('the ICO') enforces all breaches of the DPA. The ICO can impose sanctions (including criminal sanctions) against companies found to be in breach. The ICO now has the power to fine organisations up to £500,000 for a serious breach of the DPA.

16. 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.

17. Subject Access Requests under the DPA

You should also be aware of your obligations under the DPA in the event you receive a subject access request. Under the DPA individuals can ask to see information which is held about them by you (i.e. their personal data) on computer and in certain paper records. Such a request needs to be made in writing with the relevant fee as prescribed for under the DPA (£10 maximum as at January, 2014). The request should include enough information to help you find the relevant personal data. Importantly you must also satisfy yourself as to the identity of the person seeking the information, and that they are authorised to receive it. You are entitled to seek proof of identity, for example a copy of photo identification or proof of address.

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. In particular you should remember that you **may** be exempt from providing data associated with programme-making (including rushes) under 'the special purposes exemption' in accordance with s32 of the DPA – see paragraph 7 above.

You should seek to respond to a request as soon as possible but no later than within 40 days after the necessary fee has been paid. Please read the Subject Access Request Checklist on the ICO website: -

http://ico.org.uk/for_organisations/data_protection/subject_access_requests

Where the request relates to programme material including rushes, you should consult with your commissioning broadcaster before making any disclosure as there may be legitimate legal and editorial grounds for resisting disclosure.

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

18. Additional guidance and information

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

END