Responding to individuals' requests under data protection legislation: Tinopolis Group Policy

Contents

Part 1: Introduction

Part 2: Handling individual requests

Part 3: Data subject access requests

Part 4: The right to rectification

Part 5: The right to erasure

Part 6: The right to request restrictions on processing

Part 7: The right to data portability

Part 8: The right to object to automated decision-making

Appendix 1 – Acknowledgment of request / holding response

Appendix 2 – Letter to third parties regarding third party data

Appendix 3 – Substantive response to a data subject access request

Part 1: INTRODUCTION

1.1 About this document

The Data Protection Act 2018 (the **DPA**) and the give various rights to individuals with regards to the Personal Data that organisations hold about them. In this procedure, the DPA and the GDPR are collectively described as the **data protection legislation**.

This document explains the rights of individuals under the data protection legislation and provides guidance on how to handle any requests made to exercise these rights.

1.2 Purpose of this document

The purpose of this document is to set a clear procedure for employees to follow with regard to requests from individuals in order to:

- meet the provisions of the data protection legislation;
- avoid regulatory action from regulatory bodies; and
- avoid negative publicity for breaches of the data protection legislation.

1.3 Application of this document

This document applies to all employees, and should be read in conjunction with our Data Protection Policy.

It is the responsibility of all employees to read and adhere to the procedures detailed in this document. Any breach of this policy may result in disciplinary action.

1.4 Definitions used in this document

Controller – a 'person' who determines the purpose(s) and means of the processing of Personal Data. In relation to the data protection legislation, 'person' is a recognised legal entity e.g. a company or organisation; each Group company is a Controller.

Processor – any person or organisation (other than an employee or of the Controller) which processes data on behalf of the Data Controller.

DPA – Data Protection Act 2018.

Data Subject – an individual who is the subject of Personal Data.

GDPR – means Regulation (EU) 2016/679 (the General Data Protection Regulation).

Group – means Tinopolis Limited and its subsidiaries including:

- Daybreak Pictures Limited;
- Firecracker Films Limited;
- Mentorn Media Limited;
- Passion Distribution Limited;
- Pioneer Film and Television Productions Limited;

- Sunset & Vine Productions Limited;
- Tinopolis Interactive Limited; and
- Video Arts Limited.

Personal Data – any information relating to an identified or identifiable natural personal.

Third party – in relation to Personal Data means any person other than the Data Subject, the Controller or any Processor or member of staff authorised to process data for the Controller or Processor.

Part 2: HANDLING INDIVIDUAL REQUESTS

2.1 Individuals' rights

We could contravene the data protection legislation if we fail to comply with a request from an individual in accordance with their rights.

These rights are:

- to request and access a copy of the information that we hold about them. This request is commonly known as a data subject access request (**DSAR**);
- to ask for their information to be erased;
- to restrict processing of their information;
- to ask for their data to be provided in a portable format;
- to object to the processing of their information in certain circumstances; and
- to object to being subject to decisions based solely on the automated processing of their information.

More information about each of these rights is contained in the relevant sections of this document. In practice, it is likely that individuals will exercise these rights at the same time.

As a Controller, each Group company may receive requests from individual Data Subjects in accordance with their rights under the data protection legislation. We may also receive requests from third parties on behalf of Data Subjects. Each Group company must respond to valid requests in accordance with the provisions of the data protection legislation.

2.2 Practical issues for handling requests

The rights set out in the data protection legislation can generally only be exercised by the individuals themselves. We may receive requests from others (for example, parents of children, solicitors or others) but in general we cannot progress a request unless we are certain that the rights are being exercised appropriately on behalf of the individual.

We will require that the individual provides adequate identification information to ensure that we are dealing with the correct person.

Prior to 25 May 2018, we were entitled to charge a fee of £10 for responding to DSARs. However,

under the GDPR we are not able to charge for responding to any request by an individual unless it is repeated or unreasonable (see below).

2.3 **Time limits for responding to a request**

To meet the provisions of the data protection legislation, we must respond to a request without undue delay and in any event within one month of receipt of the request. This period may be extended by two further months where necessary if the request is particularly complex. However, we must still respond to the individual within one month to inform them of the delay and inform them of their right to complain to the Information Commissioner's Office.

2.4 **Dealing with repeated or unreasonable requests**

Under the data protection legislation, where a request is manifestly unfounded or excessive, in particular where it is a repetitive request, we can either choose not to respond or we can charge a reasonable fee to the individual.

It is always for us to justify that the request is manifestly unfounded or excessive, and so this should only be used sparingly and with the express agreement of the Data Protection Manager (Sara Bond). Any fee charge will be based on the administrative cost of providing the information.

Where we refuse to respond to a request, we must explain why to the individual, informing them of their right to complain to the Information Commissioner's Office and to a judicial remedy without undue delay and at the latest within one month.

Part 3: DATA SUBJECT ACCESS REQUESTS

3.1 **Recognising a DSAR**

Article 15 of the GDPR sets out the rules relating to data subject access requests. A DSAR is actually a series of rights, under which the individual is entitled:

- To be informed whether we process Personal Data relating to them;
- To be told:
    - the purposes of the processing;
    - the categories of Personal Data concerned;
    - the recipients or categories of recipients to whom the data will be disclosed;
    - where possible, the period for which the data will be stored;
    - the existence of the right to request rectification or erasure of the data;
    - the right to lodge a complaint with the Information Commissioner's Office;
    - where any information was not collected directly from the individual, any available information as to the source of the data;
    - the existence of any automated decision-making, including the logic involved in such decisions and the consequences of the processing for the individual; and
    - whether any Personal Data are transferred outside the European Economic Area and, if so, the safeguards that are in place to protect the information.
- To have communicated to them a copy of the Personal Data being processed.

Any request by an individual for all or any substantial part of the Personal Data we hold about them must be treated as a DSAR.

If an individual, for example, requests a copy of all of the information a Group company holds relating to them and the information would take considerable time require to collate, they can be asked to make a more formal written request outlining exactly what data they in order to narrow the scope of the search. This would be classed as a DSAR. This would also apply if an external company (e.g. a solicitor) requests a large amount of information while acting on behalf of an individual. An individual may restrict their request to some of the information we hold about them only.

Individuals making a DSAR will often state that they are doing so, but they are not required to do this under the data protection legislation. Individuals can make their request by letter, email, via social media or verbally. Although DSARs made on social media may be rare, we are obliged to respond to any that we do receive once we have confirmed the identity of the person making the request (see below).

We must treat any individual making a request for the Personal Data we hold about them as having made a valid DSAR that we have to comply with. If individuals make a DSAR verbally, we should ask them to make their request in writing so that we can respond formally.

3.2 **DSARs made by third parties**

A DSAR may be made on behalf of an individual by a third party. For example, an external firm or company (e.g. a solicitor) may request a large amount of information while acting on behalf of an individual and this may be a DSAR. Please note that whether a request for information is classed as a DSAR or not, employees must ensure that they do not discuss, show or release individual information to third parties who do not have permission to view that data. It is always necessary to receive written consent from the individual stating that the third party is acting on their behalf in these instances. Examples might be a written authority or a more general power of attorney. However, it is the third party's responsibility to provide this documentary evidence.

If we believe that an individual may not understand what information would be disclosed to a third party making a DSAR on their behalf, we may send the response directly to the individual rather than the third party.

3.3 **Requests for information about children**

Personal Data about a child belongs to the child rather than to their parents or a guardian. It is only the child that has a right of access to their Personal Data, even though in the case of very young children, the child's rights are likely to be exercised by those with parental responsibility.

Before responding to a DSAR relating to a child, we should consider whether the child is mature enough to understand their rights; if we are confident that they are, we should respond to the child rather than the parent. The key issue is whether the child is able to understand what it means to make a DSAR and how to interpret the information they receive as a result of this. Under the GDPR, we are obliged to ensure that we provide information to children in clear and plain language.

As a guide, the age of 12 is often quoted as the age when children can be presumed able to consent to sharing their Personal Data, but that is not an exact requirement. Please liaise with the Data Protection Manager for further guidance when dealing with any DSAR relating to a child.

3.4 **Dealing with a DSAR**

DSARs from individuals

If an employee receives a request for information from an individual, or someone acting on behalf of an individual, and they decide to treat the request as a DSAR, they must first ensure that they have the request in writing.

If an employee receives a request for data and is unsure whether it falls into the category of an official DSAR they should contact the Data Protection Manager for guidance.

When we receive a DSAR the person processing the request must contact the individual (see **Appendix 1**) making the request as soon is as reasonably practical, acknowledging the request and asking for the following (if they have not already been provided):

1. Identification information in order to verify that the person making the request is the Data Subject; and

2. If the request is being made on behalf of the Data Subject, a signed letter of authority from the Data Subject; and

3. Any further information reasonably required to enable us to locate the information sought by the individual if not already provided.

Each Group company has a duty to provide all relevant information to the Data Subject within one (1) month, starting when the individual making the request has provided us with **all** of the information listed in points 1 to 3 above. If however an individual does not respond providing us with this information, we have a duty to request the information again rather than simply treating their lack of response as an excuse not to respond to the DSAR.

Please note that we should not respond to a DSAR unless we are satisfied that the person making the request is who they say they are, or in the case of a third party we are satisfied that the third party has the Data Subject's permission to make the request on their behalf, as evidenced by the Data Subject's signed written consent.

Before supplying any information in response to a DSAR we should make sure that we have the individual's correct contact details. We can ask individuals to narrow the scope of their request, however they are not obliged to do so. The GDPR does not include an exemption for requests that relate to large amounts of data, but we may be able to consider whether a request is manifestly unfounded or excessive.

DSARs from employees

If we receive a DSAR from an employee or ex-employee of the Group, this will be dealt with by the HR department (contact: Pete Reid on Peter.Reid@Tinopolis.tv) which controls access to employee Personal Data. The DSAR should be dealt with in the same way as a DSAR relating to an individual, save that it would be inappropriate to request identification relating to a current employee who is clearly known within the Group as long as we are satisfied that they request has come from the individual we believe it has come from.

Supplying information to the Data Subject

Individuals making a DSAR are entitled to more than a copy of their Personal Data. They are also entitled to the information listed at the beginning of part 3 of this policy. These details might be contained in the information copy of the Personal Data we supply, but to the extent that they are not we will need to supply this information in addition to a copy of the Personal Data when we respond to the DSAR.

There are two points in particular to note here:

(a) individuals only have a right to know the individuals/groups to whom their Personal Data may be disclosed in general terms, they do not have a right to be given the names of those individuals/groups; and

(b) individuals need only be given an explanation of the logic behind any decision taken about them as a result of automatic processing of their data where they specifically request this.

Individuals making a DSAR are entitled to be given the information contained in Personal Data rather than the documents actually containing the Personal Data itself. Therefore, we are entitled to provide transcripts of relevant documents, print-outs of information from computer systems or copies of sections of documents containing Personal Data, rather than copies of all relevant original documents. All information must be provided in an "intelligible form". The copy of Personal Data we send to an individual in response to a DSAR should be marked: "Data Subject Copy".

Exemptions

Data protection legislation provides exemptions to our obligation to respond to a DSAR where we have a legitimate reason to do so. If one of these exemptions applies we would still need to respond to the individual making the DSAR, stating that the exemption applies so we are unable to disclose data falling within the exemption.

If you believe one of the following exemptions applies to the data in relation to which you are to respond to a DSAR please contact the Data Protection Manager for further guidance:

- confidential references;
- publicly available information;
- Personal Data processed for the purposes of the prevention or detection of crime, the capture or prosecution of offenders or the assessment or collection of tax / duty;
- data processed for management forecasting or planning;
- Personal Data that consists of a record of your intentions in negotiations with an individual where disclosing the data is likely to prejudice the negotiations; and
- Personal Data for which legal professional privilege could be claimed in legal proceedings.

In addition to considering the above exemptions, the Group will need to consider its obligations to third parties' whose Personal Data is included in the information that is supplied in response to a DSAR.

3.5 **Responsibility**

As detailed above, all DSARs received must be sent to the relevant contact within the business who will deal with it in conjunction with the Data Protection Manager. They will allocate responsibility to an individual and/or department across the Group to collate the information requested by the Data Subject.

Once all of the information has been collated, it should be returned to the relevant contact within the business for review.

3.6 **Searching for Data**

Under the data protection legislation, Personal Data which must be provided to a Data Subject when responding to a DSAR only extends to information about the individual which is processed electronically or forms part of a relevant filing system.

A relevant filing system is any set of information relating to individuals to the extent that, although the information is not necessarily processed electronically, the set is structured, by reference to

individuals, in such a way that specific information relating to a particular individual is readily accessible.

For example, a manual (i.e. paper-based) filing system whereby information is stored by individual name would be classed as a relevant filing system and would need to be searched; a manual filing system whereby individual data is stored by chronological order with no sub-dividers relating specifically to individuals would not be classed as a relevant filing system for the purposes of the data protection legislation and would not need to be searched for data in response to DSARs.

3.7 **Third Party Data**

Once the information has been collated and returned to the relevant contact within the appropriate area of the business, they must consider the Group's obligation to any third parties (e.g. another individual or a staff member) whose Personal Data which may be included in the information. The relevant business contact must check through the information thoroughly to identify whether it includes the Personal Data of any third parties. We do not have to comply with a DSAR to the extent that doing so would mean disclosing information about a third party who can be identified from that information except where:

- the third party has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without the third party's consent.

If the information contains Personal Data relating to anyone other than the individual making the DSAR, the relevant business contact must obtain the consent of the third party to the disclosure or decide whether it is reasonable to disclose the information in the absence of consent. See **Appendix 2**. When obtaining consent to disclosure from a third party, care must be taken not to disclose Personal Data about the requester to the third party. The Group must decide whether to disclose third party data on a case by case basis and cannot apply a blanket policy of withholding third party data. It will usually be unreasonable to disclose third party Personal Data, without that third party's consent.

If it is decided that the third party information cannot be disclosed when we respond to the DSAR, then it must be separated from the information to be disclosed and excluded when we respond to the request. Alternatively, if the information cannot be separated but details revealing a third party's Personal Data can be blanked out with black marker pen so that they are concealed, then this redaction should be carried out before we respond to the DSAR. Where we decide not to disclose third party information we will keep a note of that decision.

Part 4: THE RIGHT TO RECTIFICATION

4.1 **What does the GDPR say?**

Article 16 of the GDPR gives individuals the right to obtain from a Data Controller without undue delay the rectification (correction) of any inaccurate Personal Data concerning that individual. This includes a right to request that the Data Controller completes any incomplete data.

This right only applies where we both agree that the data is inaccurate. Where there is a dispute as to the accuracy of the data (for instance the individual thinks it is wrong but we think it is correct), this right does not apply. However, in these circumstances, we should record the individual's comments.

We must respond within one month to a request for rectification. This can be extended by two months where the request for rectification is complex.

Where we are not taking action in response to a request for rectification, we must explain why to the Data Subject, informing them of their right to complain to the ICO and to a judicial remedy.

Part 5: THE RIGHT TO ERASURE

5.1 **What does the GDPR say?**

Article 17 of the GDPR gives individuals the right to request for the erasure (deletion) of their Personal Data. We will only need to comply with the request and delete their data in certain circumstances. These are:

- Where the Personal Data is no longer necessary for the purpose it was being used for, and we have no other reason to keep the data;
- Where the Personal Data was being processed on the basis of the individual's consent, that consent has been withdrawn and we have no other legal basis to continue to process the data;
- Where the Personal Data was being processed on the basis of the 'legitimate interests' condition, the individual has objected to the processing and there are no overriding grounds for continuing to process the data;
- Where the Personal Data is being processed for direct marketing purposes and the individual objects to any further processing; and
- Where the Personal Data has been unlawfully processed.

We do not need to comply with a request to delete data where we are required by law to continue to hold it.

Please seek advice from the Data Protection Manager if you receive a request to delete any Personal Data.

Part 6: THE RIGHT TO REQUEST RESTRICTIONS ON PROCESSING

6.1 **What does the GDPR say?**

Article 18 of the GDPR gives individuals the right to request that a Data Controller restricts (i.e. blocks or suppresses) processing their Personal Data in certain circumstances. These are:

- Where the individual contests the accuracy of the Personal Data, for a period enabling the Data Controller to verify the accuracy of the data;
- Where the processing is unlawful, and the individual requests its processing to be restricted;
- Where the Data Controller no longer needs the Personal Data, but it is required by the individual for the establishment, exercise or defence of legal claims; and
- Where the processing is based on the legitimate interest condition, the individual has objected and the Data Controller is considering whether its legitimate interests override that objection.

Part 7: THE RIGHT TO DATA PORTABILITY

7.1 What does the GDPR say?

Article 20 of the GDPR provides a limited right for individual to receive their Personal Data, in response to a DSAR, in a structured, commonly used and machine-readable format (for example, CSV files), and to have that data transmitted to another Data Controller.

This right only applies if all three of the following conditions apply:

- The Personal Data has been provided by the individual to the Data Controller; **and**
- The processing is based on the consent of the individual or the performance of a contract between the individual and the Data Controller; **and**
- The processing is carried out by automated (i.e. electronic) means.

Information created by a Group company, or obtained from third parties, will not apply to this right.

7.2 How we will handle a request for portability

We must respond without undue delay, and within one month. This can be extended by two months where the request is complex. We must inform the individual within one month of the receipt of the request and explain why the extension is necessary. Where we are not taking action in response to a request, we must explain why to the individual, informing them of their right to complain to the ICO and to a judicial remedy without undue delay and at the latest within one month.

Part 8: THE RIGHT TO OBJECT TO AUTOMATED DECISION-MAKING

8.1 What does the GDPR say?

Automated individual decision-making is a decision made by automated means without any human involvement.

Article 22 provides a right for individuals to object to being subject to any decision based solely on automated processing which produces legal effects concerning them or otherwise significantly affects them.

Appendix 1 – Acknowledgment of request / holding response

Dear [*Data Subject*]

Acknowledgment of your data subject access request

Thank you for your [*letter/email/etc.*] making a data subject access request for [*brief description of information that has been requested*].

I am writing to let you know that we have received your data subject access request under the General Data Protection Regulation (**GDPR**). Your request was received on [*date*]. We will provide you with information without delay and, unless there are grounds for extending the statutory deadline of one month (for example, because your request is complex), we expect to be able to give you a response by [*date*].

[*I acknowledge the copy of your [specify proof of identity/address] as confirmation of your identity*.]

[*I would be grateful if you could provide confirmation of your identity and address before we proceed to compile the data you have requested.*]

In addition, please provide us with further information about the information you want. If possible, restrict your request to a particular [*production, service, department, team or individuals, incident*]. Please include time frames, dates, names or types of documents, any file reference and any other information that may enable us to locate the personal data you seek, such as emails, the names of senders and recipients, and approximate dates.

Please note that the statutory deadline for us to respond to your request may be extended by the time it takes you to provide us with the information we have requested.

Yours sincerely

[*Name*]

For and on behalf of [*Group company*]

Appendix 2 – Letter to third parties regarding third party data

Dear [*Name of third party*]

I am writing to seek your views on a request for disclosure of [*brief description of the data*].

We have received a request for disclosure. In our search we identified some records that contain personal data about you. It is our practice to seek the consent and views of any individual and to take their views into account before disclosing the information.

If you do not consent to the disclosure, we will decide whether it is nevertheless reasonable to disclose the information in the absence of your consent. Please note that the requester has the right to challenge any non-disclosure decisions we make, which means we cannot guarantee that these records will not be disclosed. However, we will ensure that your views are taken into account in any discussion about their disclosure.

The items concerned are:

- [•]
- [•]
- [•]

[*I enclose copies of them for your information*.]

Please could you let me know whether or not you have any objections to the disclosure of the items listed above? If you do have any objections, please could you explain their nature so that we can take your views into account when considering whether or not it would be reasonable to disclose them.

We are required to respond to the request for disclosure by [*date*], so I would be grateful if you could reply to this letter by [*date*].

If you would like clarification of any of the points I have raised, please feel free to contact me.

Yours sincerely

[*Name]*

For and on behalf of [*Group company*]

Appendix 3 – Substantive response to a data subject access request

Dear [*Data Subject*],

Response to your data subject access request dated [*date of request*]

We write further to your request for details of personal data which we hold.

We enclose all of the data to which you are entitled under the General Data Protection Regulation (GDPR).

We have contacted the following departments and individuals in order to locate personal data held which is within the scope of a data subject access request under the GDPR:

- [*List of departments and methodology for identifying personal data*]

We can confirm the following in relation to the data existing on the date when your request was made:

- The information that comprises personal data: [•]
- The purposes for which the personal data is processed: [•]
- The categories of personal data concerned:
- The recipients or categories of recipients of personal data to whom the data was or will be disclosed: [•]
- The envisaged period for which the personal data will be stored: [•]
- The right to request rectification or erasure of personal data, restriction of processing or objection to such processing: [•]
- The right to complain to the Information Commissioner's Office: [•]
- Any information available to us as to the source of the data: [•]
- Whether there is any automated decision-taking: [•] [*Note: Individuals need only be given an explanation of the logic behind any decision taken about them as a result of automatic processing of their data where they specifically request this.*]
- If personal data is transferred to a third country or to an international organisation, details of safeguards in relation to the transfer: [•]

[*Some names and identifying particulars have been deleted to protect the identity of third parties.]*

[*You will notice that parts of the documents have been blacked out.] [I have not enclosed all of the information you requested*.] [*This is because* [*explain why the information is exempt from disclosure*].]

Yours sincerely,

[*Name*]

For and on behalf of [*Group company*]