AEO GDPR GUIDANCE

For Event Organisers

CONNECTING THE EVENTS INDUSTRY

INTRODUCTION

The General Data Protection Regulation is due to come into effect on 25th May 2018 and will affect all organisations that hold data on individuals. If you already have robust systems that comply with the current Data Protection Act you're in a good starting position.

At the moment, the full details surrounding the new regulation and its impact on the industry are not clear* but the Live Events Promotion Group (formerly the FaceTime Working Group) will be working with ICO to provide guidance for event organisers as further information becomes available.

The main difference is that the regulation will put more onus on organisations for seeking and recording permission, being transparent about what, how and for how long data is stored and used. GDPR requires you to show HOW you comply with its principles. Larger fines will be enforced for data breaches – up to €20m or 4% of annual worldwide turnover.

If you operate internationally, you should determine which data protection supervisory authority you come under – in the UK this is the ICO (Information Commissioner's Office). The lead authority is determined according to where your organisation has its main administration or where decisions about data processing are made. For multi-site companies where decisions are made in different places this can be quite complex so it may be helpful to map out your organisation's decision making for data processing.

* Please note this is draft guidance to enable you to audit processes. More information to follow as it is released.

CONTENTS

1. WHO'S RESPONSIBLE FOR DATA IN YOUR ORGANISATION?

- Do you already have a Data Protection Officer? If not, and depending on the size of your organisation, you may want to appoint one
- Where will this role sit within your organisation's structure and governance arrangement?
- Do they have the knowledge, support and authority to take proper responsibility for your data protection compliance?
    - If you have a compliance function, responsibility for data policies and procedures may fall under this area of the business
    - Smaller organisations may wish to appoint an individual to "police" data procedures and usage within your organisation, for example, a member of the IT or marketing function, and provide specialist training in data protection
    - You may also choose to use an external data protection advisor

AEO

What do you need to do?

2.1 CONDUCT AN AUDIT

- Audit your current data procedures
    - What personal data do you hold?
    - Where did it come from?
    - How do you use it?
    - Who do you share it with?
- What parts of GDPR are likely to impact your business?
- Where are your current procedures and policies lacking in compliance?
    1. Review current privacy notices and make any necessary changes, include:
        - Easy to understand and clear language – no jargon
        - How long you will keep the data
        - That an individual has the right to complain to the ICO
        - Explain where data came from
        - Why you need it and how it will be used
        - An explanation of your legal basis for processing personal data

2.1 CONDUCT AN AUDIT

- Where are your current procedures and policies lacking in compliance?
    2. Where does data feature in your partner/sponsor contracts?
        - Do you get data from partners? Have you informed them how you will use it? Do their procedures comply with GDPR?
        - Make sure you provide partners with details of your own robust processes
    3. Identify your legal basis (conditions for processing) for the data processing you do and document it
        - Have you got a checklist for the legal basis for carrying out the various types of data processing you do?
        - People will have a stronger right to have their data deleted where you use consent as your legal basis for processing

2.2 IMPLEMENT ROBUST PROCEDURES - LAWFUL

Lawful Processing Procedure

- For processing to be lawful under the GDPR, you need to identify a legal basis before you can process personal data
- It is important that you determine your legal basis for processing personal data and document this
- This becomes more of an issue under the GDPR because your legal basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, e.g. to have their data deleted

Lawfulness of processing conditions

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public
- interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

2.2 IMPLEMENT ROBUST PROCEDURES - GOVERNANCE

Governance

- You are expected to put into place comprehensive but proportionate governance measures
- Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances
- Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data
- Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place

What is a data protection impact assessment (DPIA)

A tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

Do you need a DPIA?

- When is it necessary in your business?
- Who will do it and who needs to be involved?
- When might you need to consult the ICO?
- GDPR makes a privacy by design and data minimisation approach an express legal requirement

2.2 IMPLEMENT ROBUST PROCEDURES - GOVERNANCE

When do I need to conduct a DPIA? You must carry out a DPIA when:

- Using new technologies
- The processing is likely to result in a high risk to the rights and freedoms of individuals

Processing that is likely to result in high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal affects – or similarly significant affects – on individuals
- Large scale processing of special categories of data or personal data in relation to criminal convictions or offences
- Large scale, systematic monitoring of public areas (CCTV)

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An assessment of the risks to individuals
- The measures in place to address risk, including security and to demonstrate that you comply
- A DPIA can address more than one project

2.2 IMPLEMENT ROBUST PROCEDURES - ACCOUNTABILITY

Accountability

- The accountability principle requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility

To demonstrate that you comply you must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies
- Maintain relevant documentation on processing activities
- Where appropriate, appoint a data protection officer
- Implement measures that meet the principles of data protection by design and data protection by default
- Measures could include:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security features on an ongoing basis
- Use data protection impact assessments (DPIAs) where appropriate
- Adhere to approved codes of conduct and/or certification schemes

2.2 IMPLEMENT ROBUST PROCEDURES - ACCOUNTABILITY

If your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:

- processing personal data that could result in a risk to the rights and freedoms of individual; or
- processing of special categories of data or criminal convictions and offences

What do I need to record?

- You must maintain internal records of processing activities
- You must record the following information:
  - Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer)
  - Purposes of the processing
  - Description of the categories of individuals and categories of personal data
  - Categories of recipients of personal data
  - Details of transfers to third countries including documentation of the transfer mechanism safeguards in place
  - Retention schedules
  - Description of technical and organisational security measures
- You may be required to make these records available to the relevant supervisory authority for purposes of an investigation

2.3 UNDERSTAND INDIVIDUALS' RIGHTS

- Individual's rights - check procedures cover:
  - Subject access
    - Most cases won't be able to charge for complying with a request
    - Normally just have a month to comply (not 40 days as now)
    - Unfounded/excessive requests can be charged for or refused but will need policies/procedures in place as to why request meets a refusal
    - Need to explain your legal basis for processing personal data
  - The right to be informed – privacy notices and transparency
  - Correcting inaccuracies
  - Erasing information
  - Restrictions to processing
  - Data portability
  - Objection to processing for example blocking direct marketing
  - Prevention of profiling or automated decision-making

2.3 UNDERSTAND INDIVIDUALS' RIGHTS

- You will need to provide some additional information to people making requests such as data retention periods and the right to have data corrected
- If an individual requests any of the above, would you be able to locate and amend/delete their details easily and inform other third parties to do the same?
- Who will make the decision to delete? What impact will it have on different functions in your business?
- If you get lots of data requests it may save time and money to allow people to access their own data online

PRIVACY NOTICES

What to include:

- In order for processing to be fair, the data controller (the organisation in control of processing the data) has to make certain information available:
  - Who the data controller is
  - The purposes for which the information will be processed
  - Who it will be shared with
  - Any other information relevant to the circumstances to enable fair processing – a data audit of your organisation will help with this
  - Information about providing consent if this is what the data controller is relying on
- If explained in broad terms, a privacy notice can allow for development in how you use data whilst providing enough information on how you will use the data – but stick to definite uses not possible future uses
- Where services offered directly to a child, privacy notices must be written in a clear, plain way that a child will understand
- You may choose to go beyond legal requirements by telling people:
  - The links between different types of data collected and corresponding uses
  - The consequences of not providing data – e.g. not receiving a benefit
  - How you ensure the security of personal data
  - What you will not do with the data
- Even if you're not required by law to offer translations, it is good practice to provide your privacy notice in the language that your intended audience is most likely to understand.
- Privacy Notice Checklist

Information to supply:	Data obtained direct from subject (at time data obtained)	Data not obtained direct from subject (First communication with subject/if disclosure to a 3rd party, before the data is disclosed OR within a month of receipt of data)
Identity and contact details of the controller and, where applicable, the controller's representative, and the data protection officer	✓	✓
Purpose of the processing and the legal basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of the data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority (e.g.ICO)	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement and possible consequences of failing to provide personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓

How and where to communicate privacy notices:

- Privacy notices are not necessarily one document, they can be provided:
  - Orally - face to face or when you speak to someone on the telephone although it's a good idea to have a script and document this
  - In writing - printed media; printed adverts; forms, such as financial applications or job application forms
  - Through signage - for example an information poster in a public area
  - Electronically - in text messages; on websites; in emails; in mobile apps
  - It is good practice to provide information at collection point. So, if you are collecting information through an online form you should provide a just-in-time notice as the individual fills out the form
- Using an online privacy dashboard for complex data processing needs could be beneficial
- Privacy notices should be as clear and readable on mobile devices as on a computer screen. The text should be large enough to read so people don't have to zoom in to see it
- Rather than simply making it available for them to look for themselves, you need to actively provide privacy information in instances where an individual would not reasonably know how you will use their information
- The need to actively provide privacy information is strongest where:
  - You are collecting sensitive information
  - The intended use of the information is likely to be unexpected or objectionable
  - Providing personal information, or failing to do so, will have a significant effect on the individual
  - The information will be shared with another organisation in a way that individuals would not expect
- If you decide that you will need to actively communicate you can do this by:
  - Contacting them directly by letter or email
  - Reading out a script during a phone call
  - Providing interactive information in an online form
  - Delivering text-based notifications that appear briefly when an individual hovers over a particular field

Sharing data with 3rd parties

- It becomes complex when data is being shared between data controllers, separate privacy notices and/or a data sharing agreement will be needed in these circumstances
- Make privacy notices available to 3rd parties if selling or renting data so they can see what individuals are expecting their data to be used for and they can decide whether they need to seek additional consent to prevent a potential breach
- If a business is sold, becomes insolvent or is closed, its database can be sold on – the seller must make sure the information will only be used for a similar purpose otherwise the buyer will need to seek further consent
- If you have explicitly assured individuals that you will not share their information with third parties but now wish to do so, you should inform them and actively seek their consent. You should also update your privacy notice accordingly

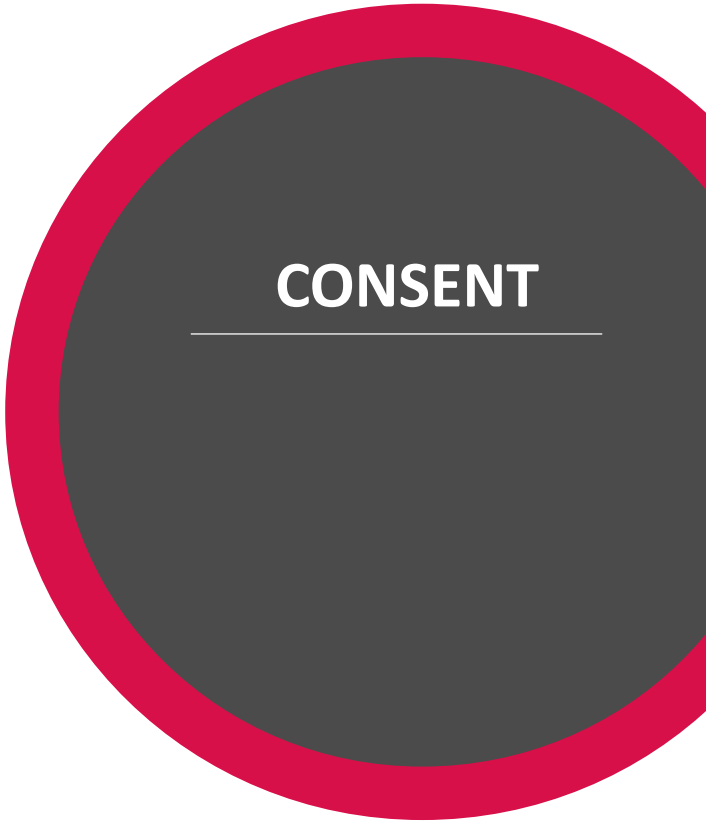
Guidance on sharing information for Direct Marketing purposes
Data Sharing Code of Practice

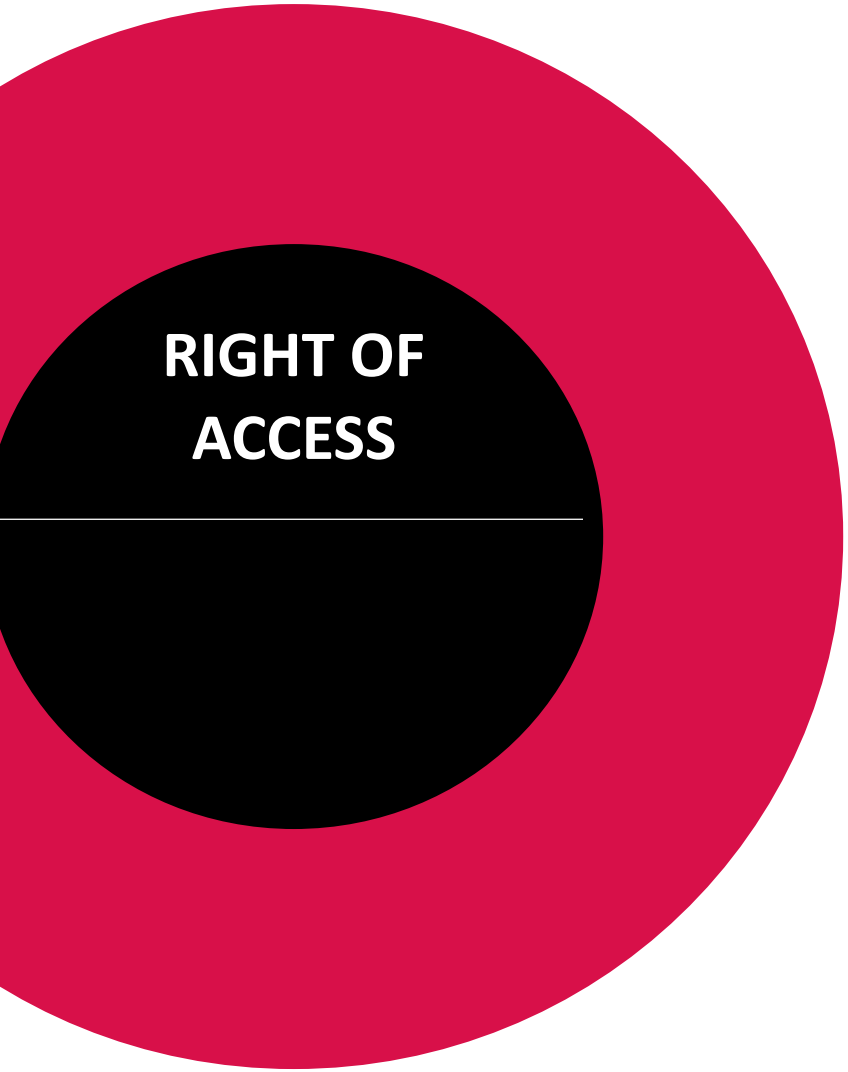
In summary you should:

- Ensure that privacy notices remain accurate and up to date
- Analyse complaints from the public about how you use their information and in particular any complaints about how you explain your use of their information
- Check that your privacy notice actually explains what you do with individuals' personal data
- Update your privacy notice to reflect any new or amended processing
- Review your privacy information regularly, particularly whenever you change or update a process to see if consent may need to be re-sought. It's important to make sure privacy notices are robust and part of ongoing business procedures so as not to be forgotten

Good and bad examples of privacy notices

- Under GDPR consent requires some form of affirmative action – silence, pre-ticked boxes or inactivity doesn't constitute consent
- If relying on consent to prove lawfulness, your method of obtaining it should:
  - Be displayed prominently and clearly
  - Ask individuals to positively opt-in
  - Provide sufficient supporting information for them to make an informed choice about providing consent
  - Explain the different ways you will use the information
  - Provide a simple way for them to indicate they agree to different forms of processing – unticked tick boxes or yes/no options
  - If seeking to use data for direct mail this should have a separate, prominent opt-in
- Some form of record must be kept of how consent was provided
- Individuals can withdraw consent at any time
- You won't need to obtain fresh consent if you have already got consent under the DPA or EC Data Protective Directive (95/46/EC) and it meets the new requirements under GDPR
- If you offer an "information society service" to children (16 and under), you will need to obtain consent from a parent or guardian to process the child's data. Member states can provide lower age as long as it's not below 13
- GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles





- GDPR clarifies that individuals should have access to their personal data so that they're aware of and can verify the lawfulness of the processing
- Individuals are entitled to:
  - Confirmation that their data is being processed
  - Access to their personal data
  - Other supplementary information that is outlined in the privacy notice
- Unlike with the current DPA, you must provide the above information free of charge, although you can charge a 'reasonable fee' based on the admin cost if requests are unfounded, excessive, repetitive or requesting copies of information already provided
- Information must be provided without delay and at the latest within a month of receipt
- If the request is complex or numerous you can extend by two months as long as you inform the individual within the initial month deadline and explain the reason for the extension
- If information is deemed excessive/unfounded you can choose to refuse to respond but you must inform the individual that this is the case and that they have a right to complain to a supervisory authority (e.g. the ICO in the UK)
- Before responding to requests you should verify the identity of the person using 'reasonable means'
- Provide information electronically if the request is made electronically
- Where possible, organisations could provide remote access to a secure self-service system

- This encompasses your obligation to provide ‘fair processing information’ emphasising the need for transparency over how personal data is used
- The importance of privacy notices should not be underestimated!
- Much of the information is consistent with the current Data Protection Act but there is some additional information required
- GDPR sets out the information you should supply and when individuals should be informed (see table under Privacy Notices)
- Information you supply should be:
    - Concise, transparent, intelligible and easily accessible
    - Written in clear and plain language, particularly if addressed to a child
    - Free of charge

RIGHT OF RECTIFICATION

- Individuals are entitled to have personal data rectified if it is inaccurate or incomplete
- If you have already disclosed the data in question to third parties it is your responsibility to inform them of the changes. You must also inform the individual about the third parties to whom the data has been disclosed
- You must respond within a month but it can be extended by two months if rectification is complex
- Where you are not taking action, you must explain why to the individual informing them of their right to complain to the supervisory authority

RIGHT TO ERASURE

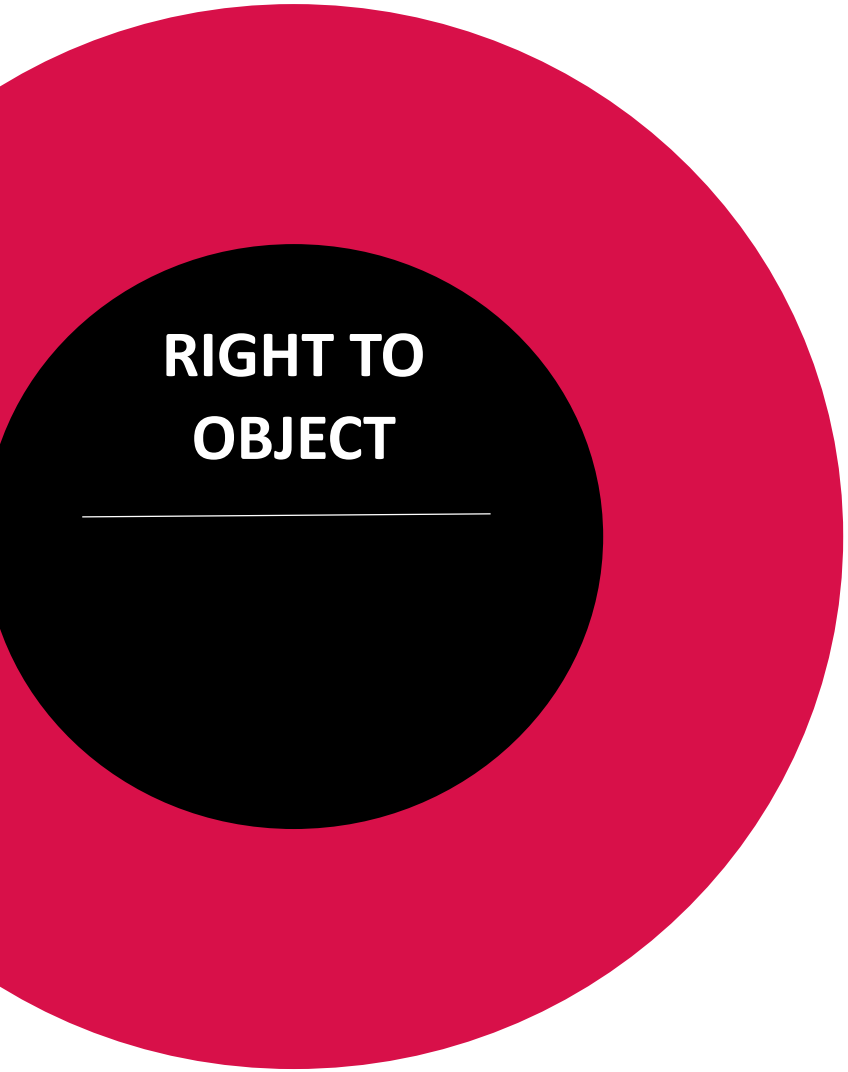
- Also known as ‘the right to be forgotten’ – it enables an individual to request that personal data is deleted or removed. Under DPA this was limited to processing that caused damage or distress but under GDPR right to erasure is valid in the following circumstances:
  - Where data’s no longer necessary in relation to the original purpose it was collected for
  - When the individual withdraws consent
  - When the individual objects to the processing and there’s no valid reason for continuing
  - The personal data was unlawfully processed (a breach of GDPR)
  - The data has to be erased to comply with a legal obligation
  - The data is processed in relation to the offer of information society services to a child
- You can refuse if the data is being processed:
  - To exercise the freedom of expression and information
  - To comply with a legal obligation for the performance of a public interest task
  - For health purposes in the public interest
  - For the exercise or defence of legal claims
  - For archiving purposes in the public interest, scientific/historical research or statistical purposes
- There are extra requirements when the erasure relates to children’s personal data – particularly if used online
- If you have disclosed personal data to third parties that is subject to an erasure request you must make them aware unless it is impossible/involves disproportionate effort to do so
- If you process personal information online e.g. on social networks, forums or websites, you must endeavour to inform other organisations who process the data to erase links, copies or replication of the data in question

RIGHT TO RESTRICT PROCESSING

- Individuals have a right to restrict processing of personal data
- If you receive a request for this you are permitted to store the data but not further process it
- You will need to restrict processing if:
  - An individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the data
  - An individual objects to the processing and you are considering whether your organisation's legitimate grounds override those of the individual
  - Processing is unlawful and the individual opposes erasure and requests restriction instead
  - you no longer need the data but the individual requires the data to establish, exercise or defend a legal claim
- You may need to review procedures to ensure you can determine where you may be required to restrict the processing of personal data
- If you have disclosed data to third parties, you must inform them about the restriction on processing unless it is impossible or involves disproportionate effort to do so
- You must inform individuals when you decide to lift a restriction on processing

RIGHT TO DATA PORTABILITY

- This 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, secure way without hindrance to usability
- Some organisations already offer services that allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to use their data to find them a better deal or help understand spending habits
- The right to portability only applies:
  - To personal data an individual has provided to a controller
  - Where the processing is based on the individual's consent or for the performance of a contract
  - When processing is carried out by automated means
- You must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. This enables other organisations to use the data
- The information must be provided free of charge
- If individuals request it, you may have to transmit data direct to another organisation if feasible, however you're not required to adopt or maintain technically compatible processing systems
- If data concerns more than one individual, you must consider whether providing the information prejudices the rights of others
- As with other rights, you must respond without delay, within a month which can be extended by another two months if complex. If not taking action you must explain why and inform the individual of their right to complain to a supervisory authority



- **Individuals have a right to object:**
  - To processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
  - Direct marketing (including profiling)
  - Processing for purposes of scientific/historical research and statistics
- **If you process data for the performance of a legal task or your organisations legitimate business:**
  - Individuals must have an objection on 'grounds relating to his/her particular situation'
  - You must stop processing data unless:
    - You demonstrate compelling legitimate grounds that override the interests, rights and freedom of the individual
    - It is for the establishment, exercise or defence of legal claims
  - You must inform individuals of their right to object in privacy notices and at point of first communication
  - This must be 'explicitly brought to the attention of the subject, presented clearly and separately from any other information'
- **If you process data for direct marketing purposes:**
  - You must stop processing data as soon as you receive an objection
  - You must deal with an objection at any time and free of charge
  - You must inform individuals of their right to object in privacy notices and at point of first communication
  - This must be 'explicitly brought to the attention of the subject, presented clearly and separately from any other information'
- **If you process personal data for research purposes:**
  - To object, Individuals must have 'grounds relating to their particular situation'
  - If you're conducting research where processing is necessary for the performance of a public interest task, you're not required to comply with an objection
- **If processing is carried out online, you must provide a means for individuals to object online**

- Identify whether your processing operations constitute automated decision making and whether you need to update procedures to comply with GDPR
- Individuals have the right NOT to be subject to a decision when:
  - It is based on automated processing
  - It produces a legal/similarly significant affect on the individual
- Individuals must be able to:
  - Obtain human intervention
  - Express their point of view
  - Obtain an explanation of the decision and challenge it
- The right DOESN'T apply if the decision:
  - Is necessary for entering into or performance of a contract between you and the individual
  - Is authorised by law
  - Is based on explicit consent
  - Does not have a legal or significant affect on someone

- **What about profiling?**
  - GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, including:
    - Performance at work
    - Economic situation
    - Health
    - Personal preferences
    - Reliability
    - Behaviour
    - Location
    - Movements
  - You must ensure appropriate safeguards are in place when profiling:
    - Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and expected consequences
    - Use appropriate mathematical or statistical procedures
    - Implement appropriate technical and organisational measures to minimise risk of errors and make them easy to correct
    - Secure personal data in a way that is proportionate to the risk to the individuals' interests and rights
  - Automated decisions must not:
    - Concern a child
    - Be based on the processing of special categories of data unless:
      - You have explicit consent from the individual
      - The processing is necessary for reasons of substantial public interest on the basis of EU/Member State law

4. BREACHES

- **What is a personal data breach?**
  - A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
- **Do you have procedures for detecting, reporting and investigating a data breach?**
  - GDPR is bringing in breach notification duty across the board – the need to inform the ICO of data breaches that are likely to cause damage such as identity theft or confidentiality breaches (in some cases the individual(s)) will also need to be informed
  - Assess your data and document which types will fall within the notification requirement if there is a breach
  - Does your team understand what constitutes a personal data breach?
  - Make sure you have an internal breach reporting procedure this will facilitate whether there's a need to inform the supervisory authority/individuals concerned
  - A failure to report a breach that could cause damage could result in an additional fine to the fine for the breach itself

4. BREACHES

- **When to notify the supervisory authority (ICO in UK)**
  - Where a breach is likely to result in a risk of the rights and freedoms of individuals e.g. result in discrimination, damage to reputation, financial loss, loss of confidentiality etc
  - A notifiable breach has to be reported within 72 hours of your organisation becoming aware of it – information can be provided in phases
- **When to notify the individual(s)**
  - Where the breach is likely to result in high risk (threshold for notifying the individual is higher than the supervisory authority)
- **Information to include:**
  - The nature of the breach
  - The categories and approximate number of individuals affected
  - The categories and approximate number of personal data records affected
  - Name and contact for DPO or other relevant contact
  - Description of likely consequences
  - A description of measures taken/proposed to deal with the breach and measures taken to mitigate adverse effects

5. DATA TRANSFER RESTRICTIONS

- **When can personal data be transferred outside the UK?**
  - Personal data can only be transferred outside the EU in compliance with the conditions for transfer set out in Chapter V of GDPR
  - Where the Commission has decided the country, territory, sector in the country or international organisation ensures adequate level of protection

- **Transfers to organisations subject to adequate safeguards:**
  - A legally binding agreement between public authorities or bodies
  - Binding corporate rules – agreements governing transfers between organisations in a corporate group
  - Standard data protection clauses – template transfer clauses adopted by the Commission
  - Compliance with a supervisory authority approved code of conduct
  - Certification under an approved certification mechanism as provided for in GDPR
  - Agreed contractual clauses authorised by the supervisory authority
  - Provisions inserted into administrative arrangements between public authorities or bodies authorised by the supervisory authority

5. DATA TRANSFER RESTRICTIONS

GDPR provides certain exceptions for transfer of personal data outside the EU if:

- Made with the individual's informed consent
- Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request
- Necessary for the performance of a contract made in the interests of the individual between the controller and another person
- Necessary for important reasons of public interest
- Necessary for the establishment, exercise or defence of legal claims
- Necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent
- Made from a register which under UK or EU law is intended to provide information to the public and which is open to consultation

5. DATA TRANSFER RESTRICTIONS

What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

Such transfers are only permitted where the transfer:

- Is not being made by a public authority in the exercise of its public powers;
- Is not repetitive (similar transfers are not made on a regular basis);
- Involves data related to only a limited number of individuals;
- Is necessary for the purposes of the compelling legitimate interests of the organisation (provided
- such interests are not overridden by the interests of the individual); and
- Is made subject to suitable safeguards put in place by the organisation (in the light of an assessment
- Of all the circumstances surrounding the transfer) to protect the personal data

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

AEO

HELPING US TO HELP YOU

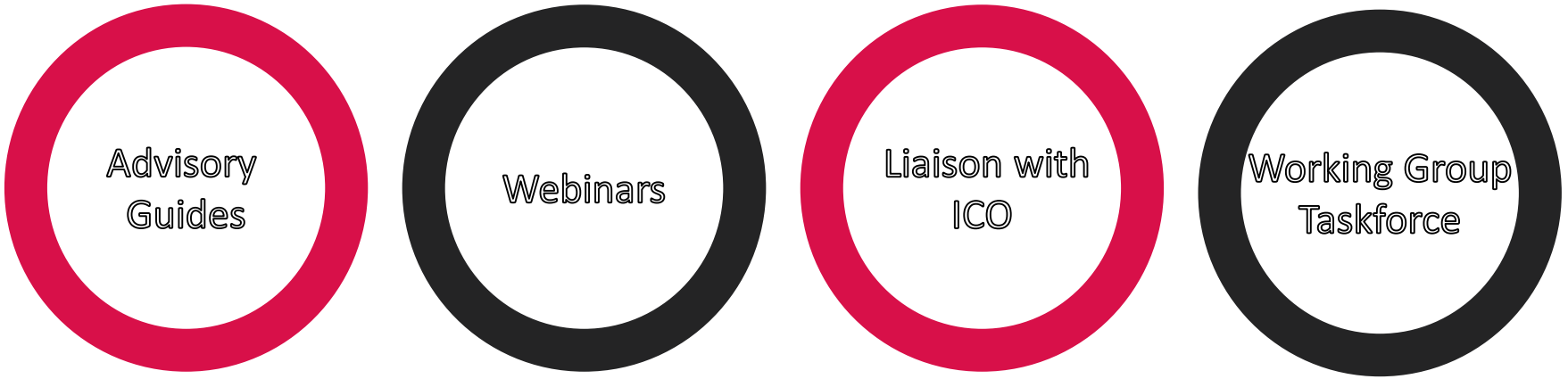
3. HELPING US TO HELP YOU

What should you be doing now?

- Information is still being released but now is the time to raise awareness throughout your organisation and put a task force together to audit your current practices, understand how your different teams acquire, store and use data and look at current procedures and policies to understand what changes will be needed
- Inform and work with the AEO, if we understand where your compliance issues are likely to be, we can work with ICO to find a solution that works for you as soon as possible so that you have time to update/change your current practices
- ICO is currently releasing documents, as and when, requesting feedback from data processors, these can be found here. If you have any feedback please let us know and we will raise it with ICO on behalf of the industry. Contact Us!

AEO - HOW WILL WE SUPPORT YOUR ORGANISATION?

We will work with our members and the ICO (Information Commissioner's Office) to understand and respond to the issues surrounding compliance with GDPR for the events industry.



AEO Ltd

119 High Street,
Berkhamsted
Hertfordshire. HP4 2DJ

Tel: **+44 (0)1442 285810**

info@aeo.org.uk