Nationwide Exhibitions Ltd Data Protection Policy & GDPR Compliance Information

version 1 – 24/5/2018

Table of Contents

Introduction

Nationwide Exhibitions Ltd (NWE) are committed to protecting the rights and freedoms of data subjects, and safely and securely processing their data in accordance with all of our legal obligations. We hold personal data about our employees, customers, suppliers and other individuals for a variety of business purposes.
This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the MD or Office Manager be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions:

Business purposes
The purposes for which personal data may be used by us:

Delivering our service, personnel, administrative, financial, regulatory, payroll and business development purposes.

Specifically, 'business purposes' includes the following:

- Delivering our services including weather related data analysis, forecasting and modelling and any other services detailed on a client's order form or contract.
- Compliance with our legal obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing new products or services
- Improving services

Personal data
'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data we gather may include but is not necessarily limited to: email address, business address, business phone number, mobile phone number, website visits, website downloads, website form entry and interactions with us (emails and phone calls).

Special categories of personal data
Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.

Data controller
'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data processor
'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Processing
'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

Our MD and our Office Manager have responsibility for the day-to-day implementation of this policy. You should contact the Office Manager for further information about this policy if necessary:

info@nationwideexhibitions.co.uk
0117 907 1000

The Principles

We shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation (GDPR). We will make every effort possible in everything we do to comply with these principles. The Principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose

Data can only be collected for a specific purpose.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up to date.

5. Retention

We cannot store data longer than necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

Accountability and Transparency

We ensure accountability and transparency in all our use of personal data.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we have done the following:

1. Reviewed all record keeping systems

2. Created a data map

3. Assessed data security measures

4. Built awareness about correct data protection with employees

5. Reviewed processes for responding to subject access requests

Data Map

The Data Map outlines how data enters the companies, where it resides, how it is transferred, how it is secured and the lawful reason for processing.

Our Procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful, in which case it will not be processed. Data subjects have the right to have any data unlawfully processed erased.

Controlling vs. processing data

NWE are classified as both data controllers and data processors. We maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing of data.

As a data processor, we must:

- Not use a sub-processor without authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If you are in any doubt about how we handle data, contact the Office Manager for clarification.

Lawful basis for processing data

All data processed by NWE has a lawful basis. We ensure that at least one of the following conditions applies whenever we process personal data:

1. Consent

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. Contract

The processing is necessary to fulfil or prepare a contract for the individual.

3. Legal obligation

We have a legal obligation to process the data (excluding a contract).

4. Vital interests
Processing the data is necessary to protect a person's life or in a medical situation.

5. Public function
Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. Legitimate interest
The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

For all existing data processing activities, the condition for lawfulness is clearly shown in our Data Map. For all new data processing activities we will a) establish that processing is necessary, and b) ensure that there is at least one lawful basis that applies to the processing purpose. This will be documented and added to our Data Map.

All individuals with data processed or held by us will be informed of the lawful basis for processing their data, as well as the intended purpose. This occurs through our Privacy Notices, Terms & Conditions and Data Protection Policy

Special Categories of Personal Data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

The company does not collect or keep any 'Special Category personal data apart from that regarding the health of employees, which is recorded solely for sickness monitoring and leave records, as explained in the internally circulated Staff Personal Data letter.

Responsibilities

Below we have listed our responsibilities that ensure data is appropriately controlled and processed.

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

NEW employee responsibilities:

- Fully understand data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

I.T:

Responsibilities that fall within the realm of IT:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one

purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. Once a request for a correction is made, we guarantee that the correction will be made within 72 hours and will be checked and documented accordingly.

Data security

General systems & cloud services:
We ensure all data we hold either on our own systems, or on cloud-based software, is as secure as possible against loss or misuse.

Third parties:
We only pass data to third parties as necessary to provide our services, or communications about our services. All third parties have been vetted for adequate security and checked for compliance with the GDPR as part of our security measures review.

Storing data securely

- We hold minimal data on paper. Hard copies of competition entry forms, Invoices payable and invoices receivable are retained by the finance department for bookkeeping purposes, and are kept for the minimum term as directed by HMRC for the purpose of submission of tax returns.

- Data stored on internal computers is protected by strong passwords that are changed regularly.

- Internal and Cloud based servers are protected by vigorous security software

- Data is regularly backed up in line with our backup procedures.

- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

- All servers containing sensitive data must be approved and protected by security software.

Data retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but each case will be determined in a manner consistent with current regulations.

Rights of individuals

Individuals have rights to their data which we respect and will comply with to the best of our ability. We ensure individuals can exercise their rights in the following ways:

1. Right to be informed

The Privacy Notice is concise, transparent, intelligible and easily accessible, free of charge, and written in clear and plain language.

2. Right of access

Individuals may access their personal data and supplementary information with a written request. Written requests should be made to info@nationwideexhibitions.co.uk

3. Right to rectification

We will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete. This will be done within 72 hours of the request.

4. Right to erasure

We will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

We will comply with any request to restrict, block, or otherwise suppress the processing of personal data.

6. Right to object

- We will respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We will respect the right of an individual to object to direct marketing, including profiling.
- We will respect the right of an individual to object to processing their data for scientific and historical research and statistics.

7. Rights in relation to automated decision making and profiling

- NWE do not carry out any automated decision making or profiling.

Privacy notices

We will supply a privacy notice at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice is provided within one month.

If the data is being used to communicate with the individual, then the privacy notice will be supplied at the latest when the first communication takes place.

If for some reason we are required to disclose information to another party, a privacy notice will be supplied prior to the data being disclosed.

The following information is included in our privacy notices:

- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information.

We will provide the individual with a copy of the information requested, free of charge, within one week of the request. We endeavour to provide data subjects access to their information in commonly used electronic formats.

Subject access requests should be directed to info@dnationwideexhibitions.co.uk

- Please include the name of your organisation, the name of the individual, your phone number, the name of your organisation's DPO or person responsible for data protection, and the data you would like to access or have deleted.

- You will then receive confirmation that we have received your request, and within 72 hours confirmation that your request has been fulfilled.

If complying with the request is complex or numerous, the deadline for fulfilling the request will be one month.

Once a subject access request has been made, we will not change or amend any of the data that has been requested.

Right to Erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, we will ensure they are contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

Third parties

Using third party controllers and processors

As a data controller and processor, we must have agreements in place with all third-party data controllers and processors that we use that ensure they are compliant with the existing regulations and that they have appropriate security measures to adequately protect the data we share with them.

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Audits, Monitoring and Training

Data audits

We will conduct data audits annually, updating our Data Map and Register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Training

All employees receive adequate training on provisions of data protection law specific to their role. If they change roles or responsibilities, they are responsible for requesting new data protection training relevant to their new position or responsibilities.

If they require additional training on data protection matters, they can contact the Office Manager

Reporting Breaches

Breach notification processes

With all data breaches, we will:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of the compliance failure(s)

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

We will report 'personal data breaches' to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in risk for the rights and freedoms of individuals. A personal data breach is defined quite widely to include: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

The notification will include the following information at a minimum:

- the nature of the breach
- the categories of data and number of people involved
- the approximate number of records
- the effect and remedial action taken

Breach notification to data subjects

We will notify affected individuals without undue delay if their rights and freedoms are put at high risk. The notification will include the following information at a minimum:

- the nature of the breach
- the likely consequences
- the measures being taken to address the breach

Failure to comply

We take compliance with this policy very seriously. Any employee who fails to comply with any requirement of this policy may be subject to disciplinary action, which may result in dismissal.