THURSBY SOFTWARE SYSTEMS, INC., GENERAL DATA PROTECTION REGULATION POLICY

Introduction

This policy is in response to changes to the law, specifically the General Data Protection Regulation (EU) 2016/679 [GDPR] (referenced by link here: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&rid=1), and the Privacy and Electronic Communications Regulation (EC) 2003 [PECR] subsequently amended (referenced by link here: Privacy and Electronic Communications Regulation (EC) 2003), which impacts on Thursby Software Systems (Thursby) as regards the processing of personal and special category data. Thursby is required to treat the personal data of those with whom it conducts its business fairly, responsibly, and in a transparent manner.

The failure of the organization, and/or employees, contractors to comply with information law could result in an investigation by the European Union's Data Protection Authorities (a list of the respective European Union Data Protection Authorities is referenced by link here: http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm).

The respective national offices responsible for data protection and information freedom, have the power to serve information, enforcement and assessment notices, issue undertakings, conduct audits, and prosecute those who commit criminal offences under the GDPR. An incident could therefore not only cause public embarrassment to, and a loss of confidence in Thursby, but would likely have financial consequences in and of themselves. In addition, where there has been a serious breach of information law, these authorities can fine organizations up to €20,000,000.

Compliance with this policy provides assurance for both the organization and individuals that personal data processed by Thursby is handled legally, effectively and efficiently, with ethical best practices at the root of decision making, in order to protect the privacy and confidentiality of our customers and those with whom we do business.

(remainder of page intentionally left blank)

Definitions

Articles 4 and 9 of the GDPR define the following key terms as follows:

| | |
|---|---|
| Personal data | Any information relating to an identified or identifiable natural person. |
| Special category data | Personal data consisting of or regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation. Additionally, while they are not considered “special category data”, children’s data and also data relating to criminal convictions are afforded further protections. |
| Data subject | An identified, or identifiable natural person. |
| Processing | Any operation (or set of) which is performed on personal data. |
| Restriction of processing | The marking of stored personal data with the aim of limiting their processing in the future. |
| Profiling | Any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a person. |
| Pseudonymization/Anonymization | Processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately. |
| Filing system | Any structured set of personal data accessible according to specific criteria. |
| Data Controller | The natural or legal person, public authority, agency or body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| Processor | A natural or legal person, public authority, agency or body which processes personal data on behalf of the controller. |
| Recipient | A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. |
| Third party | A body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. |
| Genetic data | Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. |
| Biometric data | Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data. |
| Main establishment | The place of central administration in the EU, or place where processing of personal data takes place in the EU. |
| Representative | A natural or legal person established in the EU who, designated by the controller or processor in writing, represents that controller or processor in regard to their respective obligations under the Regulation. |
| Enterprise | A natural or legal person engaged in economic activity, irrespective of its legal form. |
| Supervisory authority | An independent public authority who is established by a Member State pursuant to Article 51 of the GDPR such as the UK’s ICO. The complete list of EU public authorities and their respective representatives can be found here: http://ec.europa.eu/justice/article-29/structure/data-protection- |

| | |
|---|---|
| | authorities/index_en.htm. |
| Cross-border processing | Processing of personal data which takes place in the context of the activities of establishments in more than one Member State, or which is likely to substantially affect data subjects in more than one Member State. |
| Information society service | Any service normally provided for remuneration at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, at the individual request of a recipient of the service. |
| Purposes | Thursby processes personal data by both manual (paper) and electronic means about its employees, customers, vendors, contractors and sub-contractors, and other individuals for various purposes. The types of data, purposes for processing, and legitimizing conditions. |

Principles

To ensure our obligations under information law are met, the processing of personal information must comply with the principles of the GDPR. Accordingly, personal data will be:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject.

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’).

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

e. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

The Data Controller will be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

In line with these principles, Thursby, through appropriate management and strict application of criteria and controls will:

a. Observe conditions fully regarding the fair collection and use of information.

b. Specify the purposes for which information is used.

c. Be transparent with individuals regarding use of their personal data.

d. Collect and process appropriate information, and only to the extent that it is needed.

e. Use compliant process to fulfil operational needs while complying with legal requirements.

f. Embed policy and process to ensure information quality and accuracy.

g. Develop compliant retention processes.

h. Audit and evidence compliance.

i. Ensure that the rights of individuals can be fully accessed in line with legislation

j. Take appropriate technical and organizational security measures to safeguard personal data.

k. Ensure that any information which is transferred outside the European Economic Area is done so with legitimate purpose and appropriate safeguards.

l. Information share securely and appropriately to ensure a coordinated service provision.

m. Implement appropriate records management policy and process.

n. Implement effective risk management policy and process.

## Scope

Where Thursby acts in its capacity as a data controller, this policy applies to all employees and trustees, data processors, contractors and suppliers.

This policy covers all aspects of personal data which are processed for any purpose and by any means, by or on behalf of Thursby. It relates to personal data held both manually and electronically, and in all information-systems purchased, developed and managed by, or on behalf of Thursby.

## Employee Responsibilities

Thursby requires all employees and contractors to treat personal data with strict confidentiality, in line with data protection law. This policy is a condition of employment that staff members abide by the rules and policies as set out by Thursby. Failure to act in line this policy may result in disciplinary action.

Annual data protection awareness training is mandatory for all staff. Staff with responsibility for other areas of information compliance, such as information security and records management, may be required to undertake role-specific training.

Contractors or employees of external organizations who require access to personal data must be subject to suitable contractual arrangements, requiring them to follow the policies and processes of Thursby when handling personal data. These contractual arrangements also protect and indemnify Thursby against the improper use of personal data.

In the context of their work, employees and contractors may have access to personal data relating to visitors to our website, clients, vendors, contractors and sub-contractors, colleagues and others. Where they have concerns about data handling, or should they believe this policy has not been followed, they should raise the matter with their line manager. Their line manager should document the conversation and outcome, reporting it to the designated Data Protection Officer at the earliest opportunity.

## Management Responsibilities

### *Board of Directors*

The Trustees assume ultimate responsibility for ensuring appropriate data protection compliance within Thursby. Implementation of, and compliance with this policy is delegated to the Senior Management Team and Middle Managers.

*The Data Protection Officer*

The Thursby designated Data Protection Officer (DPO), is responsible for protecting the personal data held by Thursby, ensuring that the firm has a suitably robust information governance function, supported by appropriate policies and processes. This will include monitoring appropriate information sharing with external and collaborative agencies to facilitate coordinated provision of service. The DPO will champion Information Governance requirements and issues at the highest level within the organization.
Senior Management Team

Each member of the Senior Management Team has overall responsibility for ensuring information is handled according to the policies and processes set out by Thursby and promoting staff compliance. However, all employees are also individually responsible for ensuring that those Information Assets are handled according to data protection law and best practices, as determined by Thursby policies and processes.

*Middle Management*

Data protection processes will vary from department to department. It is the responsibility of the Middle Managers to work with the Senior Management Team, to ensure adequate and compliant processes are developed to handle personal data.

Middle Managers are responsible for ensuring a privacy impact assessment is carried out in line with Thursby' Privacy Impact Assessment Code of Practice when advised by the Support Services Director that one is necessary, or when implementing any new system, technology or procedure involving personal data.

*Data Protection Awareness*

Thursby will continue to make all staff aware of data protection through an awareness program, and awareness and compliance with this policy and the related policies and processes.

Consequences of a Breach of Policy

It is a criminal offence for a person to knowingly or recklessly without the consent of the Data Controller obtain or disclose personal data. A deliberate breach of this policy will be considered a serious disciplinary matter and dealt with accordingly. Examples of offences which may be considered gross misconduct include but are not limited to:

a. Deliberate unlawful disclosure of personal data.

b. Inappropriate use of personal data.

c. Deliberately accessing special category personal data in the absence of a legitimate business reason for doing so.

d. Misuse of personal data which results in a claim being made against Thursby.

The Lawful Basis for Processing Data.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d. Vital interests: the processing is necessary to protect someone's life.

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

f. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Contractual Obligation, Legitimate Interest and Consent

To lawfully process the personal information of an individual, Thursby relies upon contractual obligation, legitimate interest or consent. Where consent is necessary for processing, it must be explicit, freely given, specific and informed. Thursby is committed to processing personal data in a fair and transparent manner.

Where consent is relied upon as a legitimizing condition for processing:

a. Thursby will clearly and explicitly inform the data subject of all anticipated processing activities at the point of collection (or when the first contact is made if the personal data was not received from the individual).

b. Give the data subject the opportunity to consent to processing prior to undertaking the specified activity.

c. Specify a simple means by which the data subject can exercise their right to “opt out” at any time, should they wish to withdraw consent.

d. Personal data will only be processed in accordance with the activities to which the individual has consented.

Thursby has developed a series of resources to give information about privacy and data protection, and support individuals in understanding their rights and any intended processing, which data subjects will be made aware of when they give consent for us to process their personal data.

Should an individual wish that Thursby discloses personal data to a third party, such as a family member, they need to notify us of this in writing.

Disclosure of any personal data to a third party must be necessary for the original purpose for which the information was collected, and, where appropriate, undertaken with the consent of the data subject.

Data Subject Rights

The General Data Protection Regulation gives data subjects the following rights regarding the processing of their personal data. Thursby informs individuals of their information rights by

provision of our GDPR policy online both externally and internally and in privacy notices on our website.

The Right to be Informed

Thursby is committed to processing personal data in a transparent manner.

To this end, a privacy notice is available on our website. Data subjects are also provided with fair processing information and information about how to exercise their information rights at the point of first contact.

Privacy information must be provided in an accessible form, using clear and plain language, and providing all relevant information.

Where possible, Thursby will rely on contractual obligation, legitimate interest, and consent by preference in order to undertake any processing of personal data, and ensures that consent is explicit and informed. Thursby will also seek consent where possible for any disclosure of personal data to a third party, and will keep records of all such disclosures.

Thursby aims to provide data subjects with opportunities to monitor the processing of their own personal data.

The Right of Access

Under the GDPR, data subjects have the right to receive confirmation that their data is being processed, a copy of, or access to, their personal data, and other supplementary information regarding processing (including the purposes of processing, categories of personal data involved, the recipients of any disclosure, retention periods for personal data, and the existence of automated decision-making and profiling). This information must be provided free of charge, with response to the initial inquiry being given one month of receipt of the request, or receipt of confirmation of the identity of the requestor.

Subject access requests should be directed to the Support Services Director.

For further information about how Thursby complies with the right of access, see the Subject Access Process.

The Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If you have disclosed inaccurate or incomplete personal data to a third party, you must also inform

them of the rectification, if possible, and inform the individual about any third parties to whom the data has been disclosed. Rectification must take place within one month of receipt of the request, or confirmation of the identity of the requestor.
Where possible, Thursby aims to allow individuals to access and amend their own personal data. Rectification requests are dealt with by the department in which the personal data is held. If a rectification request requires further checks to be carried out, the personal data will be restricted until an outcome is determined. Proof of the identity of the person making the request, or of guardianship if they are not the data subject, will be required before a request for rectification can be actioned. Thursby keeps records of all rectification requests and their outcome.

The Right to Erasure

The right to erasure is also known as 'the right to be forgotten', which enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Following a request under the right to erase, personal data must be erased where:

a. It is no longer necessary in relation to the purpose for which it was originally processed.

b. When the individual withdraws consent.

c. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

d. Where the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).

e. It is necessary in order to comply with a legal obligation.

If the processing causes damage or distress, this is likely to make the case for erasure stronger. If you have disclosed the personal data in question to third parties, you must also inform them about the erasure of the personal data. However, there are some circumstances where the right to erasure does not apply and you can refuse to deal with a request.

Erasure requests are dealt with by a suitably trained person in the department in which the personal data is held. Proof of the identity of the person making the request, or of guardianship if they are not the data subject, will be required before a request for erasure can be actioned.

Thursby aims to comply with all right to erasure requests within one month of receipt, or receipt of proof of the identity of the requestor. Records are kept of all erasure requests and their outcome.

The Right to Restrict Processing

Under the GDPR, when processing is restricted you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in the future.

You are required to restrict the processing of personal data in the following circumstances:

a. If an individual asserts the inaccuracy of the personal data, you should restrict processing until you have verified its accuracy.

b. Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organization's legitimate grounds override those of the individual.

c. When processing is unlawful, and the individual opposes erasure and requests restriction instead.

d. If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Thursby aims to comply with the right to restrict processing through including restriction in records management, right to object and rectification processes.

Where an individual makes a request to restrict processing, it will be handled by a suitably trained person in the department which holds that individual's personal data. Proof of the identity of the person making the request, or of guardianship if they are not the data subject, will be required before a request for restriction can be actioned.

Restrictions will be put into place within a month of receipt, or within a month of receipt of proof of the identity of a requestor. If we have disclosed the personal data in question to third parties, we will inform them about the restriction of processing of the personal data.
A record of all restriction of processing requests, and their outcome, is maintained by Thursby.

## The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data 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, and when processing is carried out by automated means.

You must provide the personal data in a structured, commonly used and machine-readable form, free of charge, and within one month of receiving the request or proof of the identity of the requestor. If the individual requests it, you should transmit the data directly to another organization (if this is technically feasible).

Where an individual makes a request for data portability, it will be processed by the department which holds the subject's personal data. The individual will be required to provide proof of identity before a request for data portability can be actioned.

A record of all requests for data portability and their outcome is kept by Thursby.

## The Right to Object

Individuals have the 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); and processing for the purposes of scientific/historical research and statistics.

Where any individual objects to the processing of their personal data based on any of those grounds, you must stop unless:

a. You can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or,

b. Processing is for the establishment, exercise or defense of legal claims.

Upon receiving an objection, Thursby will immediately restrict processing of the personal data. If a determination is necessary regarding whether or not to stop processing, it will be referred to the Support Services Director. A determination will be made one month from receipt of the request, or proof of the identity of the requestor. The individual, or their guardian, may be required to provide proof of identity before an objection can be actioned.

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse. Should such a request be made, Thursby will, in a timely manner, restrict the personal data and stop processing; no determination will be necessary. Stopping processing for direct marketing purposes requests will be handled by the Sales and Marketing Manager.

We will aim to make the right to object possible through online means via the Thursby website. However, individuals can also object by contacting the department which processes their data.

A record of all objections to processing, and their outcome, is kept by Thursby.

Rights in relation to automated decision-making. Individuals have the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or a similarly significant effect on the individual. You must ensure that individuals can obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

Thursby does not undertake any decision-making based on personal data by solely automated processing. All automated processing is subject to human intervention and oversight. However, Thursby maintains a list of all semi-automated processing.

Thursby does not undertake any automated decision making using the data of persons under the age of 16.

Where semi-automated decision making must be undertaken using special categories of personal data, this is with the explicit consent of the data subject.

Where information about automated decision making is requested, it should be provided by the Services Support Director, and records of such requests and their outcome maintained. Proof of identity may be required before a person-specific response can be provided. Responses will be provided within 20 working days of receipt of the request (or proof of identity of) the requestor.

Data Sharing & Disclosure

In certain circumstances, it is appropriate that Thursby shares or discloses personal data. Where possible and appropriate, the data subject's consent will be sought prior to any sharing or disclosure.

Personal data will only be shared without the subject's consent in the following circumstances:

a. In the vital interests of the data subject or another person.

b. Where the subject lacks capacity and the data is being shared with a legal guardian.

c. Under court order or for the purposes of prevention or detection of crime.

d. Seeking legal advice or representation.

e. For the purposes of providing a confidential reference in the interests of the data subject.

f. In order to comply with a legal obligation.

If personal data will be used for legitimate business purposes by a third party, it should first be anonymized or pseudonymized. Where this is not possible, individuals will be informed at the point of collection that their personal data will be used for that purpose. Special category personal data will never be used for the purposes of legitimate business interests.

There are some partner organizations with which Thursby shares information on a regular basis. Data subjects are made aware of these organizations should it be necessary to share their personal information with them, prior to the data sharing taking place. Thursby has data sharing agreements in place with any partner organizations with which regular data sharing takes place, and takes all necessary precautions to ensure the security, integrity and proper treatment of personal data.

Where personal data will be shared with a data processor, an appropriate contractual agreement is in place which specifies how personal data may be processed, for what purposes, and under what security conditions. Such a contract sets out the obligations of both parties and indemnifies Thursby against risk in the case of the misuse of personal data by a contracted processor.

All regular, new data sharing activities are subject to a privacy impact assessment and staff will receive appropriate training should their role involve decision making regarding data sharing.

Records of all data sharing and disclosures, data sharing requests, the conditions for sharing or disclosure, and the outcomes of such activities, are maintained by Thursby.

Further information about data sharing and disclosure can be found in data sharing guidance provided by the Support Services Director.

## Information Security

Principle (f) of the GDPR states that organizations must ensure “appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures”. With continual changes to both technology and the demand for ever-easier ways by which information can be accessed and shared, it is important that a consistent approach be adopted to safeguard information.

Thursby will ensure that appropriate technical and organizational measures are in place, supported by privacy impact and risk assessments, to ensure a high level of security for personal and confidential data, and a secure environment for information held both manually and electronically.

## Records Management

Records management refers to a set of activities required for systematically controlling the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions. It is impossible to be compliant with information law without robust records management policies and practices.

Good records management practices ensure not only record quality, but that personal data is only kept for as long as necessary for its original purpose and help support data minimization. They are integral to information security methodology, and to ensuring the integrity and confidentiality of personal data. It is a key feature of risk management.

Thursby is committed to implementing robust records management policy, and best industry processes and practices to ensure compliance with the GDPR.

## Risk Management

An understanding of risk and the application of risk assessment methodology is essential to being able to effectively create a secure environment for personal data. The information held by an organization is not only one of its greatest assets, but also a potential liability. Information compliance therefore requires a proactive approach to risk management both to limit liability and protect information assets.

While it is not possible to eliminate all elements of threat, risk management aims to identify and classify risks to information systems and personal data, and find ways of mitigating, eliminating and managing those risks. In addition, it looks at ways to manage and control

incidents. It should form the backbone of all other compliance measures. With reporting regulations under the GDPR, this becomes increasingly important to insulate Thursby from sanctions and prosecution.

Thursby approaches risk management through risk evaluation and incident management processes, as well as by the use of privacy impact assessments.

May 2018

(remainder of page intentionally left blank)