itSMF UK

Data Protection Policy

May 2018

Version 1.3

itSMF UK

Introduction

Service Management Association Ltd (itSMF UK) holds personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how the Board of itSMF UK seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. This policy also applies to itSMF UK's PSMF Global platform and to its subsidiary company EssentialSM Ltd.

Definitions

Business purposes	The purposes for which personal data may be used by us: HR, administrative, financial, regulatory, payroll, membership management, marketing and business development purposes. *Business purposes include the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings* - *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, security vetting, credit scoring and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences and administration* - *Monitoring staff conduct, disciplinary matters* - *Providing services to our members* - *Marketing our business* - *Improving services*

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, members, contract and other staff, clients, suppliers and marketing contacts. *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, comments on online forums, feedback from events, supporting comments for PSMF endorsements and credits, marital status, nationality, job title, and CV.*
Sensitive personal data	*Personal data 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—any use of sensitive personal data should be strictly controlled in accordance with this policy.*

Scope

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

This policy supplements our other policies relating to internet and email use. 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 Data Protection Officer has responsibility for the day-to-day implementation of this policy. The itSMF UK Board has overall legal responsibility.

Procedures

Fair and lawful processing

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

Responsibilities of the Data Protection Officer

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging any necessary data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by itSMF UK
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Responsibilities of the Facilities/HR Manager

- Ensuring (with the assistance of Telanova) that 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

- Ensuring suitable safeguards for sensitive personal HR data.

As of February 2018, the Data Protection Officer is Mark Lillycrop (mark.lillycrop@itsmf.co.uk) and the Facilities/HR Manager is Teresa Corre (teresa.corre@itsmf.co.uk).

The processing of all data must be:

- Necessary to deliver our services

- In our legitimate interests and not unduly prejudice the individual's privacy

- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees

- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers

- Provides that customers have a right of access to the personal data that we hold about them.

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

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. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Personal data

Staff, members and partners must take reasonable steps to ensure that personal data we hold about them is accurate and updated as required. For example, if a member's personal data changes, they should update the information held within their personal profile directly or else inform the office.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on computers or portable devices (such as tablets or phones) should be protected by strong passwords that are changed regularly. All staff are encouraged to use a password manager to store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

Personal data will be retained for no longer than is necessary, taking into account the reasons that the personal data was obtained. Accounts and HR data will be retained in accordance with legal requirements. Member data (other than accounts) and marketing

data will be retained for no longer than one year after membership expiry (or the last contact with the individual concerned).

Transferring data internationally

There are restrictions on international transfers of personal data. Personal data should not be transferred outside the UK (except where existing arrangements exist, such as our US-hosted YM membership database) without first consulting the Data Protection Officer.

Subject access requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

Data subjects (staff or customers) who would like to correct or request information that the company holds about them should make a subject access request to the Data Protection Officer, who will normally respond within one month of receipt of the request. There are also restrictions on the information to which subjects are entitled under applicable law.

GDPR provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	**Transaction processing on Sage, Rapport, YM**
Who is collecting it?	Accounts team in office
How is it collected?	On-line, email and phone - no personal card details held by itSMF, just accounting records.

Why is it being collected?	To allow the organisation to deliver its services
How will it be used?	To process/collect payments for services
Who will it be shared with?	Card handlers and bank
Identity and contact details of any data controllers	Finance manager
Details of transfers to third country and safeguards	YM processing takes place in the USA; YM subscribes to Privacy Shield.
Retention period	As per legal requirements – mostly 7 years (20 years for conference exhibitor records)

What information is being collected?	**HR records**
Who is collecting it?	HR and accounts team
How is it collected?	On appointment and during employment; stored securely in print and on restricted access server
Why is it being collected?	To assist with staff selection and retention; legal requirements
How will it be used?	To help manage employee relationship
Who will it be shared with?	The individual and their line managers
Identity and contact details of any data controllers	HR manager, Finance manager
Details of transfers to third country and safeguards	None
Retention period	1 PAYE & NI - 3 years from the date of the year end they apply to. 2 Employee's financial records - 3 years

What information is being collected?	**Member data held on YM CRM system**
Who is collecting it?	Office team and member main contact
How is it collected?	Online and via email/phone.
Why is it being collected?	To allow the organisation to deliver its services
How will it be used?	To support and develop member activities
Who will it be shared with?	itSMF office team.

Identity and contact details of any data controllers	Professional services manager, marketing manager, membership team, main contact at member organisation, Preview/SOCom teams – contact via office
Details of transfers to third country and safeguards	Held in US under Privacy Shield. Profile information is under control of individual members who can also correct any errors if necessary.
Retention period	1 year after membership expiry or last contact with member, whichever is later.

What information is being collected?	**Member data held by Preview on PSMF Global microsite and Premail email system**
Who is collecting it?	Office collect email data from members for Premail. Members and endorsers provide data direct for PSMF Global.
How is it collected?	Online
Why is it being collected?	To allow the organisation to deliver its services
How will it be used?	To communicate with members on matters of interest (Premail); To support the provision of endorsements and credits to PSMF members (PSMF Global)
Who will it be shared with?	Preview Design (Premail); Freely available to access (PSMF Global)
Identity and contact details of any data controllers	Preview/SOCom teams, professional services manager, marketing manager – contact via office
Details of transfers to third country and safeguards	Some email addresses are outside UK; same safeguards will be used for all email contact
Retention period	• 1 year after last contact (Premail) • As long as member wishes to hold a personal profile (PSMF Global)

What information is being collected?	**Occasional use of mailing lists with individual consent (eg SITS opt in).**
Who is collecting it?	Third parties
How is it collected?	Via approved opt-in process

Why is it being collected?	To help the organisation to promote its services
How will it be used?	Limited email/phone contact
Who will it be shared with?	Office staff and Preview
Identity and contact details of any data controllers	Preview/SOCom teams, professional services manager, marketing manager – contact via office
Details of transfers to third country and safeguards	Some email addresses may be outside UK; same safeguards will be used for all email contact
Retention period	One year after opt-in

Conditions for processing

itSMF UK will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

itSMF UK will process personal data in compliance with all six data protection principles. The company will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that itSMF UK collects is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data 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.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the organisation to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

itSMF UK takes compliance with this policy very seriously. Failure to comply puts the organisation, its Board and staff at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.