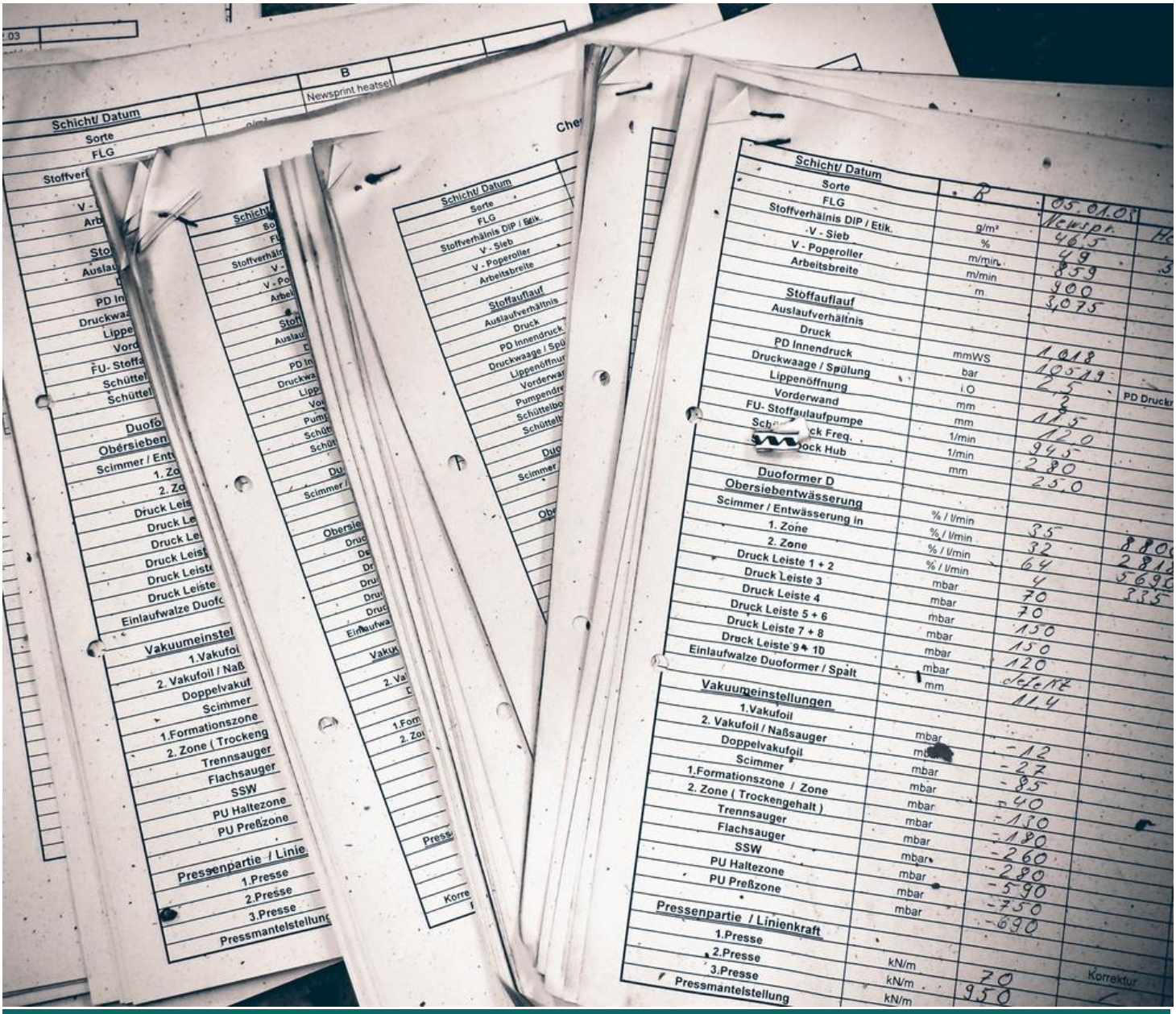

Data Protection Policy

Methodist International Centre trading as The Wesley

Audrius Pribytkovas

9/2/22

Data Protection Policy

Context and overview

Key details

- Policy Prepared by: Audrius Pribytkovas – Meeting and Events Accounts Manager
- Approved by James Barr – General Manager

Introduction

TheWesley needs to gather and use certain information about individuals. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures TheWesley:

- Complies with data protection law and follow good practice
- Protects the right of staff, customers, contractors and suppliers
- Is open to about how it stores and processes individual's data
- Protects itself from the risk of a data breach
- Process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

Data Protection Law

The Data Protection Act 1998 describes how organisations – including TheWesley – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and user fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. They say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not to be held for any longer than necessary
6. Processed in accordance with the right of data subjects
7. Be protected in appropriate ways
8. Not to be transferred outside the UK and European Economic Area (EEA), unless that country of territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to Methodist International Centre Ltd. :

- The Wesley Euston
- The Savannah Bar & Restaurant (The Wesley bar & kitchen)
- The Wesley Camden Town
- All staff of the above companies
- All contractors, suppliers and other people working on behalf of the companies listed above

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal Addresses
- Email Addresses
- Telephone Numbers
- CCTV Surveillance recordings
- plus, any other information relating to individuals

Data Protection Risks

This policy helps to protect TheWesley from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage for instance, the company could suffer is hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with TheWesley has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that TheWesley meets its legal obligations
- The James Barr – General Manager and Data Protection officer – Audrius Pribytkovas, is responsible for:
-
    - Understanding your role in relation to the personal data you are processing is crucial in ensuring compliance with the UK GDPR and the fair treatment of individuals.
    - Keeping the board updated about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule

- Within 72 hours of the data breach, reporting to Board of Directors and notifying the ICO.
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data TheWesley holds about them (also called "subject access requests")
- Checking and approving any contract or agreements with third parties that may handle the company's sensitive data
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Periodically review the data TheWesley hold, and erase or anonymise it when you no longer need it.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services
- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets like newspapers
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data process within them.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers
- TheWesley will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong password must be used, and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company or externally
- Data should be regularly reviewed and updated if it is found to be out of the date, if no longer required, it should be deleted and disposed of
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection

Data Collection

- Website Cookies – The Wesley site uses cookies to distinguish customer from other users of The Wesley site. This helps The Wesley provide customer with a good experience when customer browse The Wesley site and allows to improve The Wesley site. For detailed information on the cookies The Wesley use and the purpose for which use them, please see The Wesley Cookie Policy. If customer want to disable cookies, please refer to browser's help option.
- Automatic data capture via Wi-Fi – The Wesley hotel collects information though Wi-Fi, this policy information can be found - https://stampede.ai/company/privacy-policy/
- From Booking process -
    - Directly from you through the online booking form
    - Through the online booking channel you used to make the booking
    - From your travel agent
    - From The Wesley reservations and sales
    - From The Wesley customer made a direct booking with
- Manual data capture upon check-in or check-out
    - The Wesley location of your choice
    - Other The Wesley entities involved
    - IT service providers involved in the (online) booking process
    - IT service providers
    - Email communications service provider
- Data capture via email marketing
- Social Media

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filling cabinet
- Must be clear about what your purposes for collecting data are from the start.
- TheWesley need to record purposes as part of your documentation obligations and specify them in privacy information for individuals.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees

- If data is stored on removable media, these should be kept locked away securely when not being used
- Data should only be stored on designated drivers and servers, and should only be uploaded to an approved cloud computing services
- Servers containing personal data should be sited in a secure location, away from general office spade
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data should be protected by approved security software and a firewall.

Whilst The Wesley do our best to protect the security of information, the transmission of data across the internet and building premises is not completely secure. The Wesley cannot ensure or guarantee that loss, misuse, or alteration of data will not occur while data is being transferred.

Data use

Personal data is of no value to TheWesley unless the business can make use of it. However, is it when personal data is accessed and used that I can be at the greater risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Accuracy

The law requires TheWesley Hotel to take reasonable steps to ensure data is kept accurate and up to date.

The more important is that the personal data is accurate, the greater the effort TheWesley should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure It is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call
- TheWesley will make it easy for data subjects to update the information it holds about them. For instance, via the company website.

- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database
- It is the Head of Marketing responsibility to ensure marketing databases are checked against industry suppression files every six months.
- TheWesley should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- Must carefully consider any challenges to retention of data. Individuals have a right to erasure if you no longer need the data.
- Personal data can be kept for longer if are only keeping it for historical research, or statistical purpose.
- Children Policy - The Wesley do not knowingly collect personal information from anyone under the age of 13 (if this information collected, parent or legal guardian of child under 13 have to contact us by emailing us to mice.manager@thewesley.co.uk and we will delete that information promptly)

Data Rights

Under The General Data Protection Regulation 2018 (GDPR), everyone have several rights over their personal data.

- Informed - customer have access to this Privacy Policy on "Our" website at all times. The Wesley will continually review "Our" activities and update this policy if and when necessary. customer can contact "Our" team
- Access - customer are able to access customer information at all times. customer can do this by contacting us. The Wesley will provide customer with this information in an easily accessible format, without undue delay, and in any event, no longer than one month after receiving customer request.
- Rectify - If customer believe the personal information The Wesley hold about customer is incorrect or incomplete, customer have the right to ask us to rectify this information on customer behalf. customer can do so by contacting us.
- Erasure or the 'Right to be Forgotten' - customer have the right to have customer personal data erased where the data is no longer necessary for the purpose(s) for which it was originally collected/processed unless The Wesley have legitimate grounds or a legal right(s)/obligation(s) to store customer personal data.
- Restrict - customer can request that The Wesley restrict the processing of customer personal data if customer believe that the data The Wesley hold is inaccurate, unlawfully obtained, or customer no longer wish us to use customer personal data for any reason other than storage. Submit customer request to DPO@stampede.ai and The Wesley will respond within one month of receiving customer request.
- Data Portability - customer have the right to receive the personal data customer have provided to Us in a structured, commonly used and machine readable format.
- Object - If customer believe The Wesley are using customer information for purposes other than those customer consented to as explained above, customer have the right to object to Us using customer personal information for these purposes. Please bring this to "Our" attention by emailing us and The Wesley will identify if the activity is taking place. If so, The Wesley will cease these activities immediately.

- Freedom of Information – Subject Access Request (SAR) - customer can request a copy of the information The Wesley hold about customer (a subject access request). The Wesley will require proof of customer identity before The Wesley are able to provide customer with any personal information that The Wesley hold about customer.

Us email – Mice.manager@thewesley.co.uk

Subject access rectification requests

All individuals who are the subject of personal data held by TheWesley are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations
- Individuals have the right to access and receive a copy of their personal data, and other supplementary information.

If an individual contact the company requesting this information, this is called a subject access request.

Subject access requests from individuals can be make a SAR verbally or in writing, including on social media. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact. An individual may ask a third party (e.g. a relative, friend or solicitor) to make a SAR on their behalf. You may also receive a SAR made on behalf of an individual through an online portal. Before responding, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

If the request is from a child and TheWesley are confident they can understand their rights, TheWesley should respond directly to the child. Child may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

Request must be documented and emailed to the Data protection officer – Audrius Pribytkovas at mice.manager@thewesley.co.uk . The data protection officer can supply a standard request form, although individuals do not have to use this.

In most circumstances, you cannot charge a fee to deal with a request. Individuals may be charged up to £10 per subject access request if the request is complex or if you receive a number of requests from the individual. The data controller will aim to provide the relevant data within one month, should respond without delay and within one month of receipt of the request. TheWesley may extend the time limit by a further two months if the request is complex or if receive several requests from the individual.

The data controller will always verify the identity of anyone making a subject access request before handling over any information. Timescale for responding to a SAR does not begin until TheWesley have received the requested information.

Disclosing data for other reasons

In certain circumstances, in Schedules 2 and 3 of the Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, TheWesley Hotel will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Board of Directors and from the company's legal advisers where necessary.

The Wesley have listed below the parties to whom The Wesley may disclose client personal data for the purposes set out in this policy:

- The Wesley employees.
- Virtual hosting infrastructure providers to host The Wesley servers and data, and to provide other services to The Wesley.
- Third party consultants, service providers, or contractors when providing support and other services to The Wesley
- Auditors or advisers assisting The Wesley in "Our" business operations in any jurisdiction where The Wesley operate.

The Wesley may also disclose personal information to third parties if The Wesley are under a duty to disclose or share such data for legal or regulatory purposes, in relation to existing or future legal proceedings for the prevention of fraud/loss or to protect the rights, property and/or safety of "Our" company, "Our" customers, or others.

Refusing to comply with a request

Where an exemption applies, TheWesley may refuse to provide all or some of the requested information, depending on the circumstances. TheWesley may refuse to comply with a SAR if it is manifestly unfounded or manifestly excessive. Our detailed guidance explains the factors you should consider in determining whether a request is manifestly unfounded or excessive.

If TheWesley refuse to comply with a request, information must be provided to the individual:

- the reasons why;
- their right to make a complaint to the ICO or another supervisory authority.
- their ability to seek to enforce this right through the courts.

Providing Information

TheWesley aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

Personal Data Breach

TheWesley The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority. Data Protection officer must establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required. Must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, must also inform those individuals without undue delay.

TheWesley must also keep a record of any personal data breaches, regardless of whether you are required to notify.