GDPR & DATA PROTECTION MANAGERS TOOLKIT

General Data Protection Regulations (GDPR): The General Data Protection Regulations (GDPR) was implemented on the 25 May 2018 was the implementation where from day one, organisations are required taking steps now to ensure they comply with the new regime. GDPR applies to the McSence Group as charity and social enterprise in the same way it applies to large corporate companies. We have identified three key steps that organisations should be taking to prepare for GDPR:

- Understand what personal data you hold and process (data mapping)
- Understand the lawful basis for holding and processing each type of personal data (lawful basis analysis)
- Implement any changes to your policies and procedures to ensure compliance (implementation)

All Employees: This policy applies to all persons working for or on our behalf of the McSence Group of Companies which includes the subsidiary companies - *McSence Communication Ltd, McSence Ltd, McSence Services Ltd & McSence Workspace Ltd* in any capacity including but not limited to:

- All employees at all levels, prospective employees, agency workers, seconded workers, temporary workers, contractors/sub-contractors, clients, agents, external consultants, volunteers, members of the public, group's supply chain, third-party representatives and/or business partners who will be referred to in our Group policies as "all employees".

The Workplace: This policy applies to all persons working for or on our behalf of the McSence Group of Companies in any capacity at the workplace(s) as defined below which includes but not limited to:

- McSence Premises, Offices, Units, Business Park, Client's Premises, External Meeting Places, Customers' Homes, Gardens, Sheltered Housing, Whilst On-Call, On-Duty, Emergency Cover, Working from Home including On-Line Meetings, Whilst Driving in Company Time, Working Public Areas (café's, trains, coffee shops, buses etc) and will be referred to throughout this policy as "the workplace".
-

MANAGERS TOOLKIT

1. Data mapping: A data mapping exercise is useful to identify the personal data held by McSence Group, and the types of processing carried out in relation to that data. It helps work out the information coming in and going out of the company, as well as what happens to the data in the interim. McSence Group have set out below certain steps that we need to take:

- **Privacy notices:** At the point when personal data is obtained from an individual, they must at the same time be provided with certain information, including the purpose of and legal basis for the processing of their data. This can be done in the form of a privacy notice. Updated privacy notices should also be sent to all individuals for whom the organisation holds personal data before GDPR comes into effect.
- **Consent:** Special categories of data can only be processed with the individual's consent, such as data relating to their health. If the organisation holds data falling into one of the special categories, it needs to decide whether to destroy, return or retain the data. If retaining the data, it must have explicit written consent to do so.
- **Data subject rights:** Individuals about whom personal data is held have rights in relation to that data, including a right of access and a right to erasure. The individual has to be informed of these rights, and personnel within organisations should make sure that they have had sufficient training to understand what the rights are, when they can be enforced, and any associated time limits.
- **Contracts:** Personal data can often be passed to third parties (e.g. payroll providers). Organisations will need to make sure that the third parties that they work with are also GDPR compliant, by putting in place (or amending existing) data protection agreements with third parties.
- **Written records:** Organisations will have to maintain a written record of the processing activities they undertake, as well as those they have responsibility for but do not undertake themselves. The record will have to be available to the Information Commissioner's Office (ICO) on request.

2. Lawful Basis Analysis:

Copyright belongs to McSence Group & is not to be reproduced without McSence's permission

McSence Group understands in general terms which lawful basis is available to the group for each processing activity and, if more than one basis is available, which basis is most appropriate, given the circumstances of the organisation and the data subjects. Data processing must be within one of the prescribed legal bases under GDPR. These are listed below and there are conditions to the availability of each basis which must be satisfied:

- Processing is necessary for entering into or performing a contract with the individual.
- Processing is necessary to comply with the organisation's legal obligations.
- Processing is necessary to protect the vital interest of the individual.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation or a third party to whom the data is disclosed.
- Processing is necessary for the purposes of legitimate interests pursued by the organisation or a third party, except where such interests are overridden by the rights and freedoms of the individual.

3. Implementation: Compliance with GDPR includes compliance with six data processing principle and should be recorded in a data protection policy where personal data should be:

1) Processed lawfully, fairly and in a transparent manner.
2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Employee Data: McSence Group should retain employees' financial for at least 3 years as HMRC may request to see them in this time with the exception of payroll/HMRC which is held for 6 years. It is recommended that personal information of employees, including contact details, appraisals and reviews be kept for at least 5 years. All other data is held for no longer than 2 years after the cessation of the employment contract. Below outline the McSence Group's guidelines for the retention and disposal of employee's data:

- **Written Terms of Employment – 1 year:** Employers must retain a copy of this statement throughout the employee's employment and for one year after termination at a minimum.
- **Payroll details and Payslips – 6 years:** Records, calculations and documents relating to the value of benefits for employees must be kept for 6 years in the event of an audit by Revenue. The WRC may also inspect these in an audit and seek evidence that employees are supplied with payslips.
- **Hours of Work – 3 years:** Details of days and hours worked each week, annual leave and public holidays taken and payment received for same. Rest break records and/or records of notification of employees being fully informed about rest break entitlement and procedures if rest break is unable to be taken.
- **Maternity and Adoptive Leave Records – none:** While there is no set period of the retention of data on maternity leave or adoptive leave records, claims can be made within 6 months of employers being informed of an issue giving rise to a dispute or extended to 12 months in exceptional circumstances.
- **Parental Leave – 8 years:** Records of Parental Leave, including the period of employment of each employee and the dates and times of the leave taken, must be retained for 8 years.

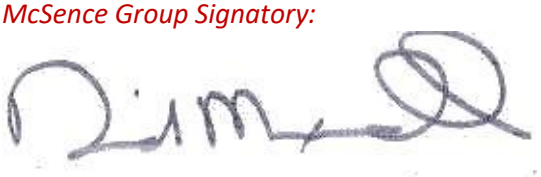
Where legislation gives no guidance on record keeping requirements, the McSence Group will carefully predetermine, and include in any employee privacy notice, how long and the grounds they will use for retaining that data. For example; an employer may decide to retain all performance review records for the entire duration of an employee's employment to monitor employee performance.

Copyright belongs to McSence Group & is not to be reproduced without McSence's permission

4. Ensuring Data Security: Appropriate technical and organisational measures have been implemented to ensure a level of security appropriate to the risk and is regularly reviewed. This includes encryption of data, restoration in the event of a physical or technical incident and ongoing assessment of security measures. McSence Group has reviewed their existing measures, and this is ongoing to determine where new measures may need to be introduced.

5. Reporting Protocol: Where there is a personal data breach, organisations should notify these to the Information Commissionaire Office without delay and, where possible, within 72 hours of becoming aware of the breach. In some circumstances, the breach must also be communicated to the individual without delay. Our data protection policy has been updating to cover our reporting protocol in the event of a data breach where appropriate reporting and communications channels have been put in place.

McSence Group Signatory:



David Maxwell
Chief Executive | McSence Group
T: 0131 454 1500 | E: mail@mcsence.co.uk | W: www.mcsence.co.uk | FB: www.facebook.com/McSenceGroup

Policy

Copyright belongs to McSence Group & is not to be reproduced without McSence's permission

SELF ASSESSMENT CHECKLIST FOR BUSINESS UNIT MANAGERS

McSence Group uses the Social Enterprise self-assessment checklist where good information handling makes good business sense and to enhance McSence Group's reputation, increase our customer and employee's confidence, and by making sure personal information is accurate, relevant and safe for the McSence Group. Business Unit Manager use the following simple checklist to improve our understanding of data protection and find out what we needed to do to make sure McSence Group keeps people's personal data secure at implementation and as we forward.

1. Do you have a record of what personal data you hold? Do you know what you use it for?

○ Yes ○ No ○ In part ***– if "No" or "In part", please refer to the "more information" section below***:

Q.1 More information:

- Have you thought about what information comes into, through and out of your business?
- Does this information include personal data about your customers? This could include names and addresses of people you deliver goods to, contacts you use for telemarketing, and members' enrolment details.
- Do you know why you collect and hold personal data?
- Have you made a record of the personal data you hold, what you do with it and why you hold it?
- Why do you hold personal data needs to fit into one of the six lawful bases for processing?

Do your records include the following information?

- The type of data you have, such as names and email addresses.
- How you got the data, such as on paper forms or through your website.
- Why you have the data.
- How long you've had the data or will keep it.
- If you share the data.
- If the data is 'special category data' or sensitive data, such as medical information.

2. Do people know you have their personal data and understand how you use it?

○ Yes ○ No ○ In part ***– if "No" or "In part", please refer to the "more information" section below***:

2. More information:

- Do you tell people how you use their personal data?
- Do you tell people if you're sharing their data?
- Do you tell people what you plan to do with their data either in paper form, such as using leaflets or posters, or online through a privacy notice or statement?

If so, does this privacy notice or statement include all the below information?

- The name of your business and the person responsible for data protection.
- Why you hold the personal data (your lawful basis) and what you do with it.
- Where you got the data from.
- Who you share the data with and how you do this, including any sharing outside the UK?
- How long you keep the data for.
- How people can request access to, or correction or deletion of, their data.
- How to complain to the ICO.
- Whether you make automated decisions or do profiling based on the data you hold.

3. Do you only collect the personal data you need?

○ Yes ○ No ○ In part ***– if "No" or "In part", please refer to the "more information" section below***:

Copyright belongs to McSence Group & is not to be reproduced without McSence's permission

Q.3 More information:

- Do you only collect the personal data you need to work with and use?
- Do you make sure people know the difference between information they need to provide and information that is optional?

For example:
Ashley is a window cleaner. He collects his customers' names and addresses, which he needs to be able to clean their windows. Ashley would also like to collect his customers' email addresses so he can email their bills instead of posting them through their front doors. As this is not necessary for him to carry out his services, he tells his customers that giving him this information is optional.

4. Do you only keep personal data for as long as it is needed?

Yes No In part ***– if "No" or "In part", please refer to the "more information" section below***:

Q.5 More information:

- Have you decided and documented how long you will hold the personal data you collect?
- Do you refresh or destroy personal data after specified periods of time?
- Do you securely delete or destroy personal data as soon as you no longer need it?

For example:
Peter is a newsagent. He collects the name, address and phone number of his customers, as well as their weekly newspaper orders and details of their payments. Peter creates a document that details what personal data he collects and how long he holds it (the retention period). At the end of the retention period, he securely destroys the data by shredding it. He also annually checks the personal data he holds to make sure everything has been deleted at the end of its retention period.

5. Do you keep personal data accurate and up to date?

Yes No In part ***– if "No" or "In part", please refer to the "more information" section below***:

More information:

6. Do you keep personal data secure?

Yes No In part ***– if "No" or "In part", please refer to the "more information" section below***:

Q6. More information:

- Do you keep personal data secure in the office, for example by using lockable filing cabinets and locking or logging off computers when away from your desk?
- Do you take steps to keep personal data secure before you take it out and about or send it somewhere else? For example, do you only take with you the data you need or send it in advance by secure methods?
- Do you keep paper documents secure, say by using lockable storage and disposing of paper records securely?
- Do you keep electronic data secure, say by encrypting mobile devices, using passwords and backing up the data?

7. Do you have a way for people to exercise their rights regarding the personal data you hold about them?

Copyright belongs to McSence Group & is not to be reproduced without McSence's permission

Yes No In part ***– if "No" or "In part", please refer to the "more information" section below***:

Q.7 More information:

Do you know about the rights individuals have under the law? In summary these are as follows:

- The right to be informed – being told what data you hold about them and what you do with it.
- The right of access – being able to request a copy of their data you hold.
- The right to rectification – being able to have inaccurate data corrected.
- The right to erasure – being able to ask you to delete / destroy their data.
- The right to restrict processing – being able to limit the amount or type of data used.
- The right to data portability – requesting to move their data electronically to another business.
- The right to object – being able to request you stop using their data.
- Do you have plans in place so you can deal with any requests?
- Do you know that a request can be made in writing or verbally, in person or on the phone?
- A request could be made over the phone, in an email, or face to face. It doesn't have to be made formally in writing by letter. If you can, treat requests that are easily dealt with as routine matters, in the normal course of business.
- For example: Simon, a local football-team manager, receives a call from a player asking for details of all the matches he has played in the last year. This can be dealt with as business as usual.
- Peter (the newsagent) is asked by a customer in the shop for the balance of her account. This can be dealt with as business as usual.
- You would probably want to treat the following requests in a more formal way:
- One of Susan's ex-employees requests a copy of the reference she gave about him to a prospective new employer.
- Kevin manages the under-10s football team and receives a request from one of the children's parents for a copy of the info held on their child.
- Do you know how long you have to respond to a request?

For example:

Pam receives a request on 3 September, so the time limit will start from the next day (4 September). This gives her until 4 October to complete the request.

However, Sachin receives a request on 30 March, so the time limit starts from the next day (31 March). As there is no equivalent date in April, Sachin has until 30 April to complete the request. If 30 April had fallen on a weekend, or was a public holiday, he would have until the end of the next working day to complete the request.

Are you able to delete someone's information if they ask you to?

Alex processes personal data to send direct marketing materials by post. As individuals may have the right to have their personal data erased, Alex makes sure he can erase personal data within one month, if needed.

8. Do you and your staff (if you have any) know your data protection responsibilities?

Yes No In part ***– if "No" or "In part", please refer to the "more information" section below***:

More information:

- Have you trained all your staff who handle personal data on their data protection responsibilities?

For example:

Bob is a builder and employs two office staff. He has briefed them about keeping information safe and secure, explained to them what privacy information he has given his clients, and told them what to do if anything goes wrong or records go missing. He also displays a poster in the office, which he printed from the ICO's Th! nk Privacy library, and does an office sweep every week to check that personal data is locked away securely.

- Do you know what to do if something goes wrong, including a personal data breach?

Copyright belongs to McSence Group & is not to be reproduced without McSence's permission

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

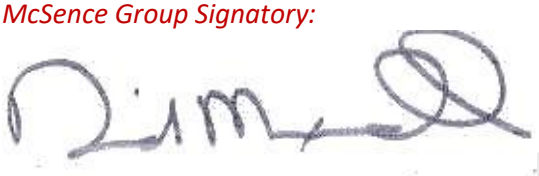
- Do you know which breaches to report to the ICO?

A breach can have a range of adverse effects on individuals, which include emotional distress and physical and material damage. You need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If a risk is likely, you must notify the ICO.

- Do you know which breaches you have to inform individuals of?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, as soon as possible.

McSence Group Signatory:



David Maxwell | Chief Executive
McSence Group - *McSence Communication Ltd, McSence Ltd, McSence Services Ltd & McSence Workspace Ltd*
T: 0131 454 1500 | E: mail@mcsence.co.uk **| W:** www.mcsence.co.uk **| FB:** www.facebook.com/McSenceGroup

***Policy Amendments & Revisions**: This policy will be reviewed annually and, if necessary, revised in the light of legislative or organisational changes Improvements will be made by learning from experience and the use of an established annual review. Should any amendments, revisions, or updates be made to this policy it is the responsibility of the Company Senior Management Team (SMT) to see that all relevant employees receive notice and training if necessary.*

Policy

Copyright belongs to McSence Group & is not to be reproduced without McSence's permission