

GDPR

Processing – Where to start?



Case Study: What is the point?

A Managing Trustee , Miss MT contacts you.

She calls you in frustration. Responsibility for data Protection at Miss MT's local church has landed on her. She strongly believes that data protection is a complete waste of time, it gets in the way of the life of the local church and is just a box ticking exercise. After getting her opinions off her chest she asks you what is the bear minimum she has to do.



Case Study

(a) What can you say to inspire Miss MT?



Case Study (a)

Suggestions:

- Caring Church
- Importance to the life of the Local Church
- Review of information held by the Local Church – is it accurate (useful)? Is it still needed? Where is it held? Is it safe?
- Respect

=> Believe in protecting personal information



Case Study



Where to start?

(b) What guidance/ tools would you point Miss MT towards?



Case Study (b)

Suggestion:

- Data Protection in a Nutshell
- 9 Steps for Methodist Managing Trustees to Take Now to Comply with GDPR
- Privacy Notice for Managing Trustees – the Annex
 - Managing Trustee Processor Record
 - FAQs



Worked example 1: 9 Steps for Methodist Managing Trustees to Take Now to Comply with GDPR

- Step 1, 2 & 9**
 - Be aware
 - Carry out a data mapping exercise (review the personal data the managing trustee body holds) and keep the results up-to-date
 - Consider data protection when making key decisions
- Step 3 & 4**
 - Provide clear and accessible information to individuals about how their data will be used (use of a Privacy Notice).
 - Understand data subject rights and accommodate these.
- Step 5, 6 & 7**
 - Identify that all processing relies on a lawful basis set out in the Privacy Notice
 - Review how Managing Trustees obtain, record and manage consent.
 - Review child data – Connexional Safeguarding Team
- Step 8**
 - Be prepared to deal with data breaches - breach workshop.



Worked example 2: Processing Record (1)

Processor and Controller details:

PROCESSOR			
Name and contact details		Representative (if applicable)	
Name of managing trustee body:	1. [[Church Council] OR [Circuit Meeting] OR [District Synod]] of [NAME OF MANAGING TRUSTEE BODY]²	Name of representative:	6. [INSERT NAME OF LOCAL CONTACT RESPONSIBLE FOR DATA PROTECTION]
Circuit/District name and number:	2.³	Address:	7. Same as managing trustee body. OR [Insert contact address for the local representative – avoid using personal/home address if possible]
Address:	3.³		
Email:	4.	Email (if different):	8.
Telephone:	5.	Telephone (if different):	9.
CONTROLLERS			
Trustees for Methodist Church Purposes Responsible for general data protection issues involving Managing Trustees arising in respect of day to day matters such as lists of members, third party users of church premises and lay employees employed by Local Churches, Circuits and Districts.		Connexional Team (registered under the name of the Methodist Church in Great Britain) Responsible for data protection matters involving Managing Trustee concerning safeguarding and complaints and discipline issues.	
Trustees for Methodist Church Purposes Central Buildings		The Methodist Church in Great Britain The Conference Office	



Processing Record (2)

Record of Processing Activities:

RECORD OF PROCESSING ACTIVITIES FOR MANAGING TRUSTEES – ARTICLE 30			
Categories of personal data:	See paragraph 2 of the Managing Trustees' Privacy Notice	Breach record:	11. See the breach record located <i>[Insert details of where this can be found e.g. in the folder marked "breach" in the locked filing cabinet in the church office or insert filename and drive if a soft copy record is filed.]</i>
Consents record:	10. See the consent record located <i>[Give details of where this can be found e.g. in the folder marked "consent" in the locked filing cabinet in the church office or insert filename and drive if a soft copy record is filed.]</i>	Retention period:	Full details of retention periods for data processed by the Methodist Church in Great Britain can be found on the Methodist Church website at: http://www.methodist.org.uk/for-ministers-and-office-holders/office-holders/archivists/
Lawful basis record:	See the Managing Trustees' Privacy Notice for details of the lawful bases identified for different types of processing and the Lawful Basis Guidance Note for reasons why these lawful bases have been selected. Details of the types of contracts, legal obligations and legitimate interests relied upon are set out in the Managing Trustees' Privacy Notice and Non-Exhaustive List of Examples .	Technical and organisational security measures:	See the general description of technical and organisational security measures set out in the Security Policy .



Processing Record (3)

Categories of Processing:

CATEGORIES OF PROCESSING		
<p style="text-align: center; margin: 0;">Categories of processing</p> <p style="font-size: small; margin: 0;">12. See Data Mapping Form for Managing Trustees, located <i>[insert details of where this can be found e.g. in the folder marked "data mapping" in the locked filing cabinet in the church office or insert filename and drive if a soft copy record is filed]</i> for details.</p>	<p style="text-align: center; font-size: small; margin: 0;">Column 1</p> <p style="font-size: x-small; margin: 0;">Transfers of personal information to countries outside of the EU or to International organisations</p> <p style="font-size: x-small; margin: 0;"><i>This column ONLY needs to be completed if the managing trustee body transfers personal information to countries outside of the EU or to international organisations e.g. if details of members were sent overseas as part of a volunteer programme.</i></p>	<p style="text-align: center; font-size: small; margin: 0;">Column 2</p> <p style="font-size: x-small; margin: 0;">Technical and organisational security measures</p> <p style="font-size: x-small; margin: 0;"><i>This column must be completed with any particular local security measures over and above those set out in the Security Policy to manage the different categories of processing listed on the left hand side of the table.</i></p>
<p>A general summary of categories of processing, taken from the Managing Trustees' Privacy Notice, is set out below. Except where indicated otherwise, these processing categories are carried out under the controllership of TMCP.</p>	<p>Names of third countries (countries outside of the EU) or international organisations that personal data are transferred to (if applicable) / Safeguards for exceptional transfers of personal data to third countries or international organisations⁵</p>	<p>General description of technical and organisational security measures (if possible)</p>
<p>A – Administration</p> <p>(1) Charity (2) Premises (3) Local Website(s)</p>		
<p>B – Contact</p> <p>(1) Incoming; Circulate contact information to allow members and non-members to contact the Church. (2) Outgoing; Contact/ engage with members and non-members about</p>		



Worked example 3 – Code of practice

Miss MT's father, Mr MT is responsible for room bookings. This already takes up a great deal of his time with people calling at all hours not to mention all the paperwork. He has contact details for all the third parties, some on his personal mobile phone, licences and booking forms since he accepted the office 8 years ago and notes of the conversations he has had with third parties over the years. Miss MT cannot face broaching the subject of data protection with her father, and asks you to talk through some of the issues with him.

- a) Could the code of practice help Mr MT to apply the general principles to his processing?
- b) What resource(s) from the data protection toolkit could help Mr MT to organise the personal information he holds?



Code of practice (Part 1)^{p9-12 of The Nutshell Guide}

1. Only collect and/or use personal information if you have a lawful reason for doing so and inform individuals about how you will use their personal information. **(Principle (a): Lawfulness, fairness and transparency)**
2. Only use the personal information that you need and only for activities relating to the life and work of the Methodist Church. **(Principle (b): Purpose limitation)**
3. Only collect and use the minimum amount of personal information that you need for a particular task. **(Principle(c): Data minimisation)**
4. Check the information you have is correct and up-to-date. **(Principle (d): Accuracy)**



Code of practice (Part 2)

5. Destroy/ delete personal information as soon as it is no longer needed in accordance with the Church's guidelines and Retention Schedule. **(Principle (e): Storage limitation)**

6. Review how you collect and store personal information in your Local Church, Circuit and District and update processes as necessary in accordance with the Data Security Policy to ensure its safety. **(Principle (f): Security, integrity and confidentiality)**

7. If you lose or allow unauthorised access to personal information, immediately contact the Appropriate Data Controller so that they can tell you what to do next. **(Principle (f): Security, integrity and confidentiality)**



Code of practice (Part 3)

8. Respond to requests to exercise data rights e.g. To erase information or provide details of information held without delay and notify the Appropriate Data Controller. **(Ch III GDPR: Data Subject's rights and requests)**

9. Take responsibility for complying with the principles and demonstrate compliance through having appropriate processes and records in place. **(Accountability principle)**



Questions?

