Macclesfield & Congleton District Scout Council

GDPR Compliance Procedures

V1.0 August 2018

Author: Martin Taylor
Owner: District Data Controller - Macclesfield & Congleton District Scout Council
Representative: District Commissioner Mark Eden

Purpose of this Procedure

These procedures describe what processes need to be Owned and Controlled by the Data Controller (DC) to assure General Data Protection Regulation (GDPR) compliance within the District.
They describe how to execute:

1. Creation of a GDPR compliant system vs a specific data set (in this case, the Personal Data held by the District)
2. Normal operation of GDPR activities to create, update, report, use and delete data
3. Exceptional processes such as Subject Access Requests, Deletion Request, Data Breach procedure and how to deal with existing Historical records

Its scope covers storage and manipulation of all personal data for Explorer Scouts, Network Scouts and other adult District staff (Uniformed, Executive and Administrative) as described in the Data Privacy Policy.
These procedures must be maintained and circulated to DPs, as recorded in the District GDPR analysis sheet by the Data Controller.
Note: A data set is Owned by its Data Controller (DC), and updated/managed by Data Processors (DPs) appointed by the Data Controller. (The DC may also allow him/herself to be a DP).

In this document, “DC” always refers to Data Controller, NOT District Commissioner!

Processes covered

Setting up the GDPR Compliance system (one off activity)
Gaining permission to store data
Transferring data
Creating/Updating Records
Deletion of Data, destruction of paper records
Subject Access Request
Data Breach procedure
Using Email, Spreadsheets and other common electronic tools
Handling Paper Records
Handling Multiple Copies of Records
Dealing with Historical data (one off activity)

Setting up the GDPR compliance System

The following activities are necessary to ensure compliance with GDPR when setting up a compliant System for managing personal data

(Note: System = People + Processes + Procedures +Facilities (secure physical stores, shredders etc) + Computerised Applications + Other Media e.g. paper records).

Step	Activity	Who
1.1	Identify Data Controller (DC)	Macclesfield & Congleton District Scout Council
1.1.1	Appoint a representative of the DC (REP):	EXEC
1.2.1	Prepare Data Privacy Notice	REP
1.2.2	Agree Data Privacy Notice	Exec
1.3.1		REP
1.3.2	Review Data Analysis sheet with interested parties	Exec, Leaders, Treasurer, etc
1.3.3	Finalise/Approve Data Privacy Policy (ensure it has a version number and date, and "lock" it by producing a ".pdf" copy)	REP
1.4.1	Identify Data Processors (DPs) and add to Data Analysis Sheet. These will typically be Leaders (for uniformed Sections) and District Processors for non-uniform staff	REP
1.4.2	Ensure logical Security of Electronic Applications (e.g. Compass, OSM, Spreadsheets, email) is adequate	REP
1.4.3	Ensure physical Security for long-term paper storage is available, and short-term physical security practices are documented (in these Procedures)	REP
1.4.4	Appoint "Lead" DP(s) to administer access rights to computerised applications (e.g. Compass, OSM), to enable control over who (DPs) have access to these applications, and to ensure that auditing of these can take place.	REP
1.4.5	Ask Lead DPs to set up access rights for all DPs on computerised applications (OSM, Compass etc)	REP to request, DPs to do
1.4.6	Ensure that Data Privacy Permission Form and Data Privacy Procedures reflect each other, and are available to DPs	REP
1.4.7	Ensure DPs, as listed in the Data Analysis sheet, have all read the Data Privacy Policy and Procedures, and completed a GDPR Permission Form	REP
1.4.8	Store DP Permission Forms in the long-term paper storage location	REP
1.5	Ensure DPs, as listed in the Data Analysis sheet, comply with the data retention schedule and securely delete/ destroy data in a timely fashion.	REP

Gaining permission to store data

Step	Activity	Who
2.1.1	Ask for Data Privacy Policy + Permission form to be circulated to all current members, and future members as they join	REP to request, DPs to do

2.1.2	Send DP notice and Permission Form to new members	DPs
2.1.3	Gather responses, return adult forms to District Administrator, keep youth member forms with Unit paperwork for Explorers and Network. Adult permission forms to be stored in the District GDPR physical repository	DPs Dist Admin to file adults' forms
2.1.4	Store returned forms securely	REP, DPs
2.1.5	Review data stored and securely delete or destroy it in line with the data retention process	REP

Note: permission to hold data for members who have left is not required, but deletion of some/all of this historical data may be necessary – see "Dealing with Historical Data" below.

Transferring data

When a young person moves section, their previous DP may hold personal data about them. It may be possible to pass this data to the new DP, in some cases electronically, possibly even direct from one data set to another in the same application (e.g. Scout moves to Explorers with data on OSM).

Step	Activity	Who
3.1.1	On receiving new member who has completed a Permission Form, ask whether their old Section holds records, whether it is ok to transfer these, and who is the DC/DP for the old section. If ok, carry out steps 3.1.2 and 3.1.3	DP
3.1.2	Approach the previous DC/DP and request a copy of this data (not originals)	DP
3.1.3	New DP to update data stores and old DP delete the transferred copy of information where able to do so under legal obligations	DP

Creating/Updating Records

Step	Activity	Who
4.1.1	DP(typically Section Leader or District Administrator) to request access details from Lead DP for computerised systems and identify secure (locked, strong) storage for paper records	DP
4.1.2	Obtain information to set up, amend records – this may be: - New joiner information on paper, email or other electronic medium - Attendance records - Training/badge data - Contact Details - Sensitive personal information - Events data - Request to update/correct data from the person who signed the permission form (and no-one else!)	DP
4.1.3	Transcribe data accurately onto the approved systems, visual check after entered	DP
4.1.4	Delete/securely destroy original copy of data (email, paper, .pdf or other file etc) unless it is a document for which the Analysis sheet specifies a retention period (typically documents requiring a signature)	DP

Deletion of Data

Deletion of data in a fully compliant GDPR system is not simple. It is essential that locations of the different Record Types, especially for paper records, is clearly stated in the Data Analysis sheet.

Step	Activity	Who
5.1.1	Delete/securely destroy data when a member leaves, in accordance with the Data Analysis sheet retention periods	DPs
5.1.2	Delete/securely destroy data on request from the person who signed the Permission form (and no-one else!)	DPs
5.1.3	Periodic check the Data Analysis sheet every year (minimum) and delete electronic records, destroy paper records in accordance with destruction schedule, especially looking for data relating to people who have left the section.	DPs

Subject Access Request

In GDPR terminology, the "Subject" is the person to whom data relates. Any Subject, or their parent if under 13, who has signed the Permission form, is entitled to see data stored relating to them in ALL media, applications and paper stores. This is called a "Subject Access Request" (SAR).

Step	Activity	Who
6.1.1	On receipt of an SAR, check that this has come from the person who signed the Permission form (and no-one else!) and the scope of data being requested is clear	DP
	Send to the requester within 72 hours either an acknowledgment of their request informing them that their request will be dealt with within the legal deadlines (one month unless complex) or inform them that more information is required to complete the SAR or decline their request explaining why i.e. not the person on the Permission form.	DP
6.1.2	Log the SAR in the SAR Log Tab of the District GDPR Analysis Sheet, including date received and requester details. File a hardcopy of the actual request in the District GDPR physical repository	DP
6.1.3	Extract all requested data relating to a Subject from OSM and/or other electronic media, and also paper stores (camp attendance lists, Gift Aid forms, accident books, etc) For adult members requesting Compass data, instruct them to access this themselves in the first instance	DP DP/ Requester
6.1.4	Scan paper forms, ensuring that only information relating to the subject is visible. This may require support from the DC.	DP(with REP support)
6.1.5	Send to the SAR requester within one month from receipt of all the required information, the information they have requested, noting that queries about the data should be directed to the DP, who may need to consult the DC and their rights to complain to the Information Commissioners Office with contact details.	DP

Data Breach procedure

A Data Breach is an incident where it is strongly suspected or known that personal data has been released in an uncontrolled way (e.g. Application or email account has been hacked, laptop containing spreadsheets has been hacked or stolen, filing cabinet has been broken into).

Step	Activity	Who
7.1.1	Anyone detecting a potential Data Breach to identify the relevant DC and report it immediately. Prompt action is imperative as DCs are under a legal duty to report relevant breaches to the regulator, The Information Commissioner, within 72 hours of becoming aware of the breach.	Anyone detecting a potential Breach
7.1.2	Secure the data (e.g. take Applications offline by contacting 3rd party support agency), physically re-securing paper etc	REP supported by DPs
7.1.3	Record the Data Breach time reported, scope of data loss, scope of Subjects affected in the Data Breach Log Tab of the District Analysis sheet, and store detailed records relating to the breach in the District GDPR physical repository	REP supported by DPs
7.1.4	Where legally required Report Data Breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach	REP supported by DPs

7.1.5	Notify the person who signed the permission form of potentially affected Subjects	REP supported by DPs
7.1.6	Take advice and act on instruction from ICO	REP and DPs

Using email, Spreadsheets and other common electronic tools

Some tools, such as Email and Spreadsheets, are extremely useful, but require a little thought to ensure we are GDPR compliant. Below are some rules to follow when mentioning people in Email or Spreadsheets – these are not exhaustive, please try to use these as a basis for using other electronic tools too.

Step	Activity	Who
8.1.1	Laptops, computers, tablets, phones etc used to process personal data must be password protected	REP and DPs
8.1.2	Email accounts must be password protected	DP and anyone who sends Scouting related email
8.1.3	Attachments that contain names with personal data must be at least password protected ideally encrypted – otherwise, as soon as they are downloaded to a PC or phone, they will be visible. Passwords for attachments to be transmitted in a different transaction, preferably via a different medium from the file itself. E.g., send a password protected file as an email attachment, then send the password by SMS message or phone call	DP and anyone who sends Scouting related email
8.1.4	Emails containing personal data to be stored as part of the GDPR System (i.e. transcribed to e.g. OSM/Compass, or to a paper record) must be deleted once the transcription is complete, including emptying the wastebasket in your email system	DP
8.1.5	Spreadsheets containing personal data should be password protected (in Excel look for Save As, Tools, General Options, password protection)	DP

Handling Paper Records

Paper records may be difficult to manage, so their use should be minimised. They cannot be easily modified or searched, and individual data items or records cannot easily be removed from them, so items containing multiple Subjects such as registers will be difficult to manage. However, there are tasks which cannot be managed electronically, so paper has its place.

Step	Activity	Who
9.1.1	Ensure that the “Location” for each paper record type is listed in the Data Analysis spreadsheet	REP
9.1.2	Ensure that paper records are written legibly, and that the event, activity or other topic is clearly stated, with date.	DPs
9.1.3	Ensure that records of the same type are filed together in sequential order	DPs
9.1.4	Where a paper record relates to a single subject, this must be shredded when deletion is due. Where a paper record relates to multiple subjects (e.g. attendance registers) these must be shredded when all Subjects’ data has been deleted.	DPs

Handling Multiple Copies of Records

It is sometimes necessary to make several paper copies of data from either an electronic or paper master (e.g. spreadsheet or paper listing of who will attend an event), perhaps to schedule Scouts into an activities roster and give a copy of who is due when, to each activity base. Or a different "cut" of data may be needed to ensure that campers who require medication actually receive it. These are perfectly valid reasons for making copies of data, but each of these is then another Personal Data form which must be controlled as described below.

Step	Activity	Who
10.1	Activity Leader (e.g. NAP holder) to consider the need for copies, the minimum number required, who will hold them, and whether those people are suitably aware of the importance of controlling personal data.	Event Leader
10.2	Create the required copies, marked as "return to or confirm deletion of this form when the activity has finished" and distribute them as late as reasonably possible to identified individuals, with instructions to keep them safe.	Event Leader
10.3	Check that copies have all been securely destroyed, as soon after the event as possible.	Event Leader
10.4	If information from Applications is sent out for update (e.g. membership lists from OSM/Compass pre-census) these copies of information should be sent securely (see section on Email and Spreadsheets) with instruction to delete the copy Email/File once processed.	DP

Dealing with Historical data (one off activity)

Historical Personal Data is data which relates to Subjects who have left the Section.
Note that some historical information (e.g. Camp attendance lists, Gift Aid forms) may be required to be kept for some years before deletion. Although we don't necessarily have permission to store these from the time they were created, Scout Association advice is that we do not need to go back now and get permission.

Step	Activity	Who
11.1	Identify Historic data held, by Type, against the Data Analysis sheet	REP with DP support
11.2	Secure any electronic information on a Password protected PC, or in a secure physical store	REP with DP support
11.3	Assess retention of each Type vs the Data Analysis Sheet, and delete/destroy any data which is older than the lifetime specified in the Data Analysis sheet	REP with DP support