Data Protection Officer Service Action Plan

As your Data Protection Officer (DPO), we will undertake an annual data protection compliance review. The review is split into 13 key areas, and we will give you an overall compliance score, as well as a rating of high, medium or low risk for each section. This plan highlights some of the key factors for each section that we will look at during the review. We strongly encourage you to get started on some of the points in this Action Plan before our visit, as this will significantly improve your compliance position.

The sections covered in the review are:

1. Governance
2. Accountability
3. Privacy Notices
4. Lawful basis and the use of consent
5. Data Protection Impact Assessments (DPIAs)
6. Record of Processing Activities (RoPA)
7. Third party data processors
8. Data Breaches
9. Subject Access Requests (SARs)
10. Training & Awareness
11. Excessive processing and unauthorised disclosure
12. Information Security
13. Retention & Disposal

(1) Governance

The organisation should ascertain what **policies** are currently in place in relation to Data Protection.
We have template policies covering:

- Data Protection (including an *appropriate policy document* covering Special Category Personal Data)
- Data Breaches
- Records Management (including a Retention Schedule)
- Information Security
- CCTV

These can be adopted by the organisation individually or combined into a Data Protection Handbook. These are the policies that we recommend you use and using them will save you time. These templates, along with other documents, are all available on the members area of our website.

The organisation should also have **procedures and guidance** in place covering:

- SARs (see also Section 9 – procedures are often included within the policy – see above)
- Breaches (see also Section 8 – procedures are often included within the policy – see above)
- Working offsite
- Bring Your Own Device (BYOD) – use of personal/unmanaged devices for processing organisational data
- Clear desks
- Locked screens
- Cyber security awareness
- Malicious emails

Many of the above sometimes feature in a Staff Acceptable Usage Policy.

(2) Accountability

The organisation should:

- Provide regular updates to its stakeholders (Mgmt Board/Trustees) on the organisation's compliance position.
- Provide training and awareness to it senior stakeholders (eg SLT/Mgmt Board) on their roles and responsibilities
- Document any data protection risks (ideally in a risk register) along with any treatments (mitigations) and monitor the mitigations
- Include any data protection issues arising from any recovery actions in its Business Continuity Plan
- Ensure staff are made aware of data protection policies (at least annually)
- Have an explicit approach to data protection complaints, including a form (ideally electronic) for submitting them, acknowledgement within 30 days, measures taken to investigate, and the complainant kept informed throughout

Data Protection Officer Service Action Plan

Trustees/Mgmt Board should be setup with organisation email addresses and be instructed to only process organisation data within this mailbox and any portals that might be setup for sharing minutes/agendas etc. Mgmt Board/Trustees should also be reminded that emails are formal records and therefore within scope of requests made under FOI (for organisation data) and DPA (for personal data).

(3) Privacy Notices

The organisation should ensure it has **Privacy Notices** in place (which are designed for transparency/informing and not for approval or for gaining consent for processing) for all personal data processed. Typically, notices would cover:

- Customers / Clients / Residents / Children / Young People
- Workforce (Board members, Trustees, staff, contractors, and volunteers)
- Job Applicants
- Visitors
- Website / Cookies

These notices should be **clearly signposted** or included in the appropriate place. For example, the Privacy Notice for applicants should be included in the application form or included on the vacancies page of the organisation's website and referenced on the application form. Privacy Notices should be regularly updated (where new processing, sharing, retention occurs) and should be in plain, easy to read language. It is also recommended to (a) **signpost the notices** for Customers/Residents and the workforce to these audiences **on an annual basis**; and (b) **reference the relevant Privacy Notice on all forms which collect personal data.**

We also have templates covering the above.

(4) Lawful basis and use of consent

The RoPA (Section 6) will highlight the lawful basis for processing (under UK GDPR). Where **consent** is used as a lawful basis for processing, it must be **freely given**, **specific** to the processing activity, **informed**, **unambiguous** (via a clear opt-in), and as easy to withdraw as it is to give.

Consent is often used for processing **images for promotional purposes, for the use of any biometric systems, and the use of marketing cookies on the website**. Therefore, the organisation should ensure it can evidence consent for these activities. It is recommended to split consents for the use of photos to those activities which are internally facing (eg pictures on display boards within offices) and those which are externally facing (eg organisation website/social media, and press). Any forms should also reference the relevant Privacy Notice(s). Please note images retained on your main internal systems for identification/safeguarding purposes should not be processed on the basis of consent.

The organisation should ensure it has provided customers/residents/staff with regular opportunities to review/withdraw consent – these details should be included on the form which collects the consent(s), as well as annual reminders sent out to say they can review their consent options at any time (and how they would do so). The organisation should manage consents centrally and staff should check this central register each time a photo is to be used.

(5) Data Protection Impact Assessments (DPIAs)

The organisation must build in **data protection by design** at the start and throughout any new processing initiatives involving personal data. If the processing is high risk (systematic processing of special category data, eg safeguarding systems, or surveillance, eg CCTV) then a **Data Protection Impact Assessment (DPIA)** should be completed and sent to the DPO for review/sign off). We have a suite of templates available for certain processing activities (eg CCTV) which should help when completing these. DPIAs must be reviewed annually alongside the DPO.

(6) Record of Processing Activities (RoPA)

Article 30 of the UK GDPR requires public bodies to maintain a Record of Processing Activities (**RoPA**). This records **all** the processing activities and the subsequent purposes.

The RoPA will also need to include:

- the lawful basis for processing (GDPR Articles 6 and 9),
- the category of data (eg personal or special category),
- the retention period (which can link to your Retention Policy),

- whether it is shared with or processed by a third party.

Whilst this area appears complex, there are **templates** available which will assist you in this area.

The RoPA also adds value by identifying any commercial efficiencies that can be made (i.e. multiple systems), include indicators of where AI processing is apparent, when responding to incidents/breaches (data flows), and when processing SARs (identifying data sources).

(7) Third Party Data Processors

The completion of the RoPA (Section 6) will highlight any **third-party data processors** or organisations where data is shared on a data controller to data processor basis. Where third parties are processing on behalf of/on instruction from your organisation, they will be classed as **data processors**. In these instances, a **Data Processing Agreement** will need to be in place. Typically, these sit within contracts and agreements, but they can be separate. The contracts/agreements should be checked to ensure they contain the standard data protection contract clauses (we have a template Data Processing Agreement).

The organisation will also need **assurances** from the third parties as to their compliance position, as well as understanding whether any personal data is transferred outside of the UK/EU.

(8) Data Breaches

The organisation must provide regular **training and awareness to staff** so they understand what a data breach and a near miss may look like. The organisation should **foster a culture of reporting** breaches ASAP and not of staff fearing reprisal. The organisation should **log both data breaches and near misses** (the DPO will too), but the organisation's log should be used to **identify any local trends** where measures can be implemented to stop an actual breach from happening (from reviewing near misses) or implement measures to reduce the likelihood of a similar incident from happening again (from reviewing breaches). The **DPO should be informed of all breaches** (no matter how serious). **Lessons learned from breaches should be disseminated to staff.**

(9) Subject Access Requests (SARs)

The organisation must provide regular **training and awareness to staff** so they understand what a SAR may look like. **Staff must know the process to follow for a SAR** (ie send to the DP lead in the organisation who may contact the DPO for advice). The organisation must have **procedures and resources in place to deal with SARs** (see Section 1 for guidance/procedure). The DPO has a *SAR Guide* which key staff within the organisation should be familiar with.

(10) Training and awareness

The organisation must ensure **all staff and trustees/Board Members** who process personal data have received data protection training. Therefore, it is recommended the organisation develop and maintain a programme of training and awareness.

We would recommend that alongside formal annual training (which should also be documented on CPD logs), **staff meetings/briefings** are used to discuss day to day issues and the measures to be implemented. **Awareness posters** should also be considered.

In terms of **induction**, new staff should be briefed on the location of the policies, the expected day to day measures to be implemented, the existence of the data protection lead and the organisation's DPO. Content for training and awareness should be taken from any **previous incidents/breaches**, as well as the organisation's **risk register**, and the views/topics of the DPO. The DPO has training video's available to use and can also attend formal training days/twilight training sessions (there may be a nominal charge for this).

(11) Excessive processing and unauthorised disclosure

This area is covered by a **walk round risk assessment**. If staff complete these it is recommended to combine with any Health and Safety Risk assessments that may occur. We have a Check List available for you to use (whilst we are conducting visits remotely) which includes the below. However, elements to look out for would be:

- Ensuring clear desk principles are maintained when areas are left unsupervised or when leaving for the day
- Cabinets locked which contain sensitive data (eg HR, Safeguarding, Medical Data)
- Ensuring personal data is not left on display

- Visitor Books – can you see other's data?
- Allergy/Medical data – Can anyone onsite access this? (balancing security and availability)
- Are devices locked when unsupervised?
- Are sensitive meetings in an all staff calendar? If so, they should not include the individual's name/initials
- Are screens facing areas where unauthorised disclosure can occur? (eg windows/hatch where parents/public can see in)
- Do prints simply come out of the printer or is code entry/badge release in place?
- Are telephone callers verified before any disclosure of information?
- Ensure personal data is not kept outside of its retention period
- Are archive boxes clearly marked with destruction dates?
- Are systems able to auto delete data after its retention period?

(12) Information Security

The organisation should ensure it obtains **assurance** on its IT security measures that are currently in place. The DPO has an IT security Questionnaire which can be provided to the organisation's IT Lead. The DPO will then assess the return and make any necessary recommendations. Areas commonly recommended are:

- Devices (such as laptops) are encrypted
- Multi factor authentication is enabled for remote access (eg O365, remote portals)
- Robust backup and restore arrangements are in place
- Systems and software are regularly patched/updated
- Un-supported operating systems/software are migrated to current (supported) versions
- Technical security – antivirus/malware, MFA, DMARC/DKIM/SPF (for anti-spoofing of emails)
- Permissions don't allow for software to be installed/executed (except for IT Admins)
- Password complexity requirements are in place
- Restrictions on the number of failed logins are in place
- Policies covering the use of personal/unmanaged devices (aka BYOD) are in place (if the organisation allows BYOD)
- A Cyber Incident Response Plan (CIRP) is in place and has been tested/exercised
- Onsite server room is secured

(13) Retention and Disposal

The organisation should ensure:

- It retains records in line with its retention schedule (usually found within its Records Management Policy – see Section 1).
- Any onsite archives are secured, and boxes indexed with a destruction date.
- A formal file structure is in place to allow for records to be easily located and managed.
- It disposes of personal data in a secure manner.
- Where external third parties are utilised, the organisation should ensure the provider disposes of data to a certain standard and provides the organisation with **certificates of disposal** (this includes any IT assets).

On a day to day level, the organisation should ensure it has **confidential waste bins** available for staff to use, and that these are secure **'post box style'** bins (not open top), and that staff are briefed on what is expected to be disposed of in confidential waste, and what can be disposed of in the normal recycling/waste.

Any storing of waste for collection by a third party should also be **logged** (so the organisation can account for all bags) and secured appropriately (eg in a locked area/cupboard). If the organisation uses shredders, these should be to **DIN-3 (cross-cutting) standard** - with the waste then disposed of in the recycling.