The General Data Protection Regulation and associated legislation

Part 3: Workbook for Community Pharmacy Greater Manchester (CPGM)

Workbook for CPGM (March 2026)

Community Pharmacy
GDPR Working Party

Contents

Template A: Decide who is responsible

CPGM

CPGM is the data controller and is responsible for data protection and implementation of the GDPR.

Responsible for GDPR compliance: CPGM Services and Contractor Support Lead – Adrian Kuznicki

IG Lead: CPGM Board Member - Ifti Khan

Data Protection Officer (if required)
(add name and contact details)

The DPO may, or may not, be a member of staff. The DPO has responsibilities set out in the GDPR – guidance may be found in the Information Governance Alliance's guidance '*The GDPR Data Protection Officer*' at https://www.digital.nhs.uk/article/1414/General-Data-Protection-Regulation-guidance. The DPO should advise you on your obligations under the GDPR and should have expert knowledge of data protection law. You may want to appoint a DPO even if you are not required to do so.

NB: Business data is not subject to the GDPR – but some 'business data may also be personal data and subject to the GDPR; and,
Anonymous data (e.g. statistical data) is not personal data but pseudonymised data is personal data even if you do not have the key or information to identify the data subjects.

Template B: Action Plan

Please refer to CPGM GDPR Action Plan Checklist Spreadsheet

Data protection impact assessment	N/A
DPO appointed, if applicable	N/A
Relevant ICO number	ZA212770
Paid current annual fee to the ICO	Yes

Adrian Kuznicki and IG Lead have signed off the policies and procedures in this workbook and related policies and procedures.

(Name, date and sign)	Ifti Khan – 12/03/2026
Annual review date	March 2027

Template C: Think about and record the personal data you process;
Assure your lawful basis for processing

Activity: records of contractors and other contacts used for the work of the LPC including NHS mail accounts

LPC status	Data Controller
Data subjects and personal data	Personal data such as name, address and contact details that may be part of business data (business data is not subject to the GDPR).
Purpose	LPCs must be able to communicate with their contractors as part of the wider management of the NHS.
Lawful basis for processing personal data	Article 6(1)(f) of the GDPR. Necessary for the performance of a task in the public interest **or** Article 6(1)(f) the legitimate interests of the LPC. Data is also processed on the basis of a consent model e.g. Contractors can sign up to the CPGM newsletter.
Special category of personal data	N/A
Basis for processing special category of data	N/A
How is data collected?	As appropriate from contractors, CPE, NHS England, NHSBSA, Primary Care Support England, Commissioners and overarching management teams for LPCs (most such data is business data in the public domain and not subject to the GDPR, but some data may be personal data and subject to the GDPR).
How is data stored?	**Via CPGM server**: • CPGM SharePoint • Access Database • Excel • MS Forms • Office 365 Outlook **External Third Party Websites/systems** • MailChimp • PharmOutcomes (Via GMHSCP license) • WhatsApp • Eventbrite • Choice Voting
How long is data stored?	Whilst contractor in place, until notified otherwise by NHS BSA. e.g. while the individual is a contractor or connected with a contractor or no longer an appropriate contact or if we are requested to delete any information by the contractor.

To whom do you provide the data (recipients)? (including processors)	As appropriate to contractors, CPE, NHS England, NHSBSA, Primary Care Support England, Commissioners and overarching management teams for LPCs (most such data is business data in the public domain and not subject to the GDPR, but some data may be personal data and subject to the GDPR).
Date confirmed that this applies to your LPC	February 2026

NB. Much of CPGM contractor data is likely to be business data and not personal data and, therefore, not subject to the GDPR.

Template C continued

Activity: VOIP phone system to process incoming/outgoing calls to/from CPGM Office team

LPC status	Data Controller
Data subjects and personal data	Business calls to/from CPGM office team to/from CPGM stakeholders.
Purpose	LPCs must be able to communicate with their contractors as per the responsibilities outlined in the LPC constitution.
Lawful basis for processing personal data	Article 6(1)(f) of the GDPR. Necessary for the performance of a task in the public interest **or** Article 6(1)(f) the legitimate interests of the LPC.
Special category of personal data	N/A
Basis for processing special category of data	N/A
How is data collected?	Office team details held on 8x8 admin console including name and email address. Incoming outcoming calls are not recorded. However, voicemails are recorded via the 8x8 app/server. No voice recordings are taken.
How is data stored?	Office team details stored on 8x8 admin console. Voicemails are set to automatically forward to users email and then automatically delete from 8x8 server.
How long is data stored?	Office team details held on 8x8 admin console until an office team member leaves the business. Voicemails are automatically deleted once forwarded to users email address.
To whom do you provide the data (recipients)?	External stakeholders can leave a voicemail if they choose to. Alternatively, users have the option to hang up.

Date confirmed that this applies to your LPC	February 2026

Template C continued

Activity: Employment records

LPC status	Data Controller
Data subjects and personal data	Personal data relevant to the employment including employee name, address, contact details, bank details and relevant financial details, contacts and reference numbers, staff appraisals, contracts.
Purpose	Employment purposes – and tax and National Insurance purposes.
Lawful basis for processing personal data	Article 6(1)(e) of the GDPR, necessary for the performance of a task in the public interest **or** Article 6(1)(c) necessary for the performance of a contract.
Special category of personal data	Yes, health data and DBS checks, as appropriate.
Basis for processing special category of data	Article 9(2)(h) of the GDPR (including the Data Protection Act). 'The provision of health care or treatment' or 'the management of health care systems or services or social care systems or services' or 'necessary for reasons of public health in the area of public health'.
How is data collected?	From employees and referees; job application, interview form, holiday and sick notes; appraisals and complaints against.
How is data stored?	HR folder on OneDrive for confidential data & payroll, Staff folder on SharePoint for holiday bookings, emergency contacts. Hard copies in locked filing cabinet in the office. This information is also stored on YouManage Servers. YouManage for employees holiday booking and sickness.
How long is data stored?	Term of employment – archived after term and removed after 7 years.
To whom do you provide the data (recipients)? (including processors)	Processor: Payroll – kath@proudgoulbourn.secure-comm.com Processor: CPE (LPC members and employees data) Recipients: HMRC, Employees & Member's Banks, NEST pensions (or others if opt out – none do at present) Processor: CCGs, LAs, NHS England, GMHSCP – for adding to relevant communication channels. Processor: Ellis Whittam (Employment Advice)
Date confirmed that this applies to your LPC	February 2026

Template C continued

Activity: Enhanced and other local commissioned services – data concerning health - list if/as relevant.

LPC status	Data Controller
Data subjects and personal data	Pseudonymised personal data that **excludes** the patient name, address and contact details but **includes** medicines and relevant health data. The key to identify patients **is not** held by the LPC.
Purpose	Care of the patient, pharmacy payment and NHS management.
Lawful basis for processing personal data	Article 6(1)(e) of the GDPR, necessary for the performance of a task in the public interest **or** Article 6(1)(f) the legitimate interests of the LPC.
Special category of personal data	Yes, data concerning health (this could include information on a disability). The data may also be another special category of personal data.
Basis for processing special category of data	Article 9(2)(h) of the GDPR (including the Data Protection Act). 'The management of health care systems or services or social care systems or services' or 'necessary for reasons of public health in the area of public health'.
How is data collected?	Specific to the local service; details included in the service specification.
How is data stored?	Within PharmOutcomes, Neo or for some services.
How long is data stored?	Specific to the local service; details included in the service specification.
To whom do you provide the data (recipients)? (including processors)	Specific to the commissioner of the service; details included in the service specification. The processor may be for example PharmOutcomes.
Date confirmed that this applies to your LPC	February 2026

Template C continued

Retention of records

The following may be helpful in considering retention periods:

A copy of the NHS guidance – the *Recommendations for the Retention of Pharmacy Records – prepared by the East of England NHS Senior Pharmacy Managers 2019*
Recommendations for the Retention of Pharmacy Records - prepared by the East of England Senior Pharmacy Managers – 2012 (cpsc.org.uk)

Records Management Code of Practice for Health and Social Care 2016
https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016

Records may be kept for longer periods than the legal minimum retention period. The retentions periods used should be retained as part of the workbook included in each Template C.

Common Law Duty of confidence (confidentiality)

The common law duty of confidence (confidentiality) continues to apply to healthcare practice and the courts have recognised three broad circumstances under which confidential information may be disclosed:

- consent – whether express or implied (implied consent means that the subject knows or would reasonably expect the proposed use or disclosure and has not objected)
- authorised or required by law, for example under statute, common law (including duty of care) or legal proceedings.
- Overriding public interest, for example where a patient is contagious or the public is at risk, such that there is a public interest in disclosure that overrides the public interest in maintaining confidentiality.

(This is a partial quote from the Information Governance Alliance (IGS) booklet on Guidance on Lawful Processing.)

Responsibility for Processing Personal Health Data

Under the GDPR, a healthcare professional (such as a pharmacist or a pharmacy technician subject to registration and regulatory oversight), social work professional or a person with a duty of confidentiality under a legal provision, must be responsible for the processing of data concerning health.

Template D: Process according to data protection principles

To process personal data in accordance with data protection principles you must have suitable policies in place. The policies supporting the Data Security and Protection Toolkit (DSPTK) are listed at the end of this workbook and you may have many of these already. These will be added to or amended by (the templates in) this booklet and the other guidance documents (Part 1 and 2).

Following the data protection principles involves for example:

Principle	**Issues to consider**
Lawfully	All your processing is lawful – templates C and F Also, responsibilities, DPO, action plan, ICO fee and sign off – templates A and B
Fairly and transparent	A privacy notice is provided, any objections to processing are considered and data breaches dealt with appropriately – see templates G, I, J and K Also, processors' contracts are appropriate – see template E
Adequate, relevant and limited for the purposes	Personal data available only to those who need to see it for the work they do – privacy by design and default apply and Data Protection Impact Assessments are carried out if required – see templates L and M Also, processors' contracts are appropriate – see template E
Accurate/up to date	Records are accurate and, if relevant, up to date – see template H (Data Quality)
Form in which identification kept for no longer than necessary	Pseudonymisation/redaction of personal details, has been considered, as appropriate – consider privacy by design and default – see template L
Security	There is appropriate physical, electronic and human security – see template H
Integrity	Data is backed up so that it is protected against accidental loss or damage – see template H

Template E: Review and check with your processors

Identify your processors and ensure that your **contracts** with them are GDPR compliant.

Your existing contractual terms may already comply, your first step should be to check this or seek clarification from your processors.

Your processors may include your clinical IT systems suppliers, PMR intermediate aggregator company, any person providing data capture and reporting systems (such as PharmOutcomes), any external body that undertakes your payroll for you.

List your processors and confirm any assurances sought and received.

Processor, product and service	**Date assurances requested**	**Date confirmation received from processor**	**Date contract ends**
Proud Goulbourn	12/01/2026	Privacy Irlam, Manchester : Proud Goulbourn	No end date
CPE	12/01/2026	Our Privacy Notice - Community Pharmacy England (cpe.org.uk)	No end date
Mailchimp (Newsletter)	12/01/2026	General Data Protection Regulation (GDPR) Compliance: Get GDPR Consent for Marketing | Mailchimp	No end date
YouManage	12/01/2026	Youmanage Privacy Policy | Your Privacy Is Important to Us	No end date
PharmOutcomes	12/01/2026	Help - PharmOutcomes	No end date
Microsoft	12/01/2026	Microsoft Privacy Statement – Microsoft privacy	No end date
8x8	12/01/2026	8x8 Privacy Notice | 8x8	No end date
Eventbrite	12/01/2026	Eventbrite Privacy Notice	No end date
Choice Voting	12/01/2026	Privacy Policy | Choice Voting Online STV Voting	No end date

You should be able to rely on your processors to provide you with the necessary guarantees listed on the next page.

You may only use those processors providing sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR and ensure the security of the data and that you can meet any data subject right.

Your processors should be cross-checked with your information asset register which lists your pharmacy hardware and software.

You are likely to be a processor for other data controllers, in which case you may have to provide information and assurances to them.

The ICO indicates that contracts with processors:

Must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Must also include as a minimum the following terms requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

More information is available from the ICO, but we would expect your processors to ensure that their contracts with you are GDPR compliant.

Template F: Obtain consent if you need to

Note: LPCs have a lawful basis for processing personal data because of the performance of a task carried out in the public interest or legitimate interests of the LPC (Stage 1). This should include your processing your contractor and other healthcare contacts, including NHS mail accounts, as part of, for example, the provision of information by CPGM, such as the CPGM Newsletters. (The processing of pseudonymised health data is (stage 2) for the management of health or social care systems).

For other activities, you may need to obtain consent for the processing of personal data.

Consent
If you process personal data lawfully by consent, from 25th May 2018, the consent must be GDPR compliant **and** recorded.

'Consent' of the data subject under the GDPR means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent gained by pre-ticked consent boxes is not valid consent under the GDPR.

If you process a special category of personal data (such as data concerning health) by consent, you must have the **explicit consent** of the patient/data subject.

Explicit consent is intended to be more specific than 'consent', and must be confirmed in words, rather than by any other positive action i.e. the person giving consent must signal agreement to an explicit statement in words such as 'I consent to emails about your products and special offers' (followed by a tick box to be completed, or not, as the case may be).

If you collect personal data for marketing purposes, you should read the ICO's guidance on consent.

Filing system / activity	**GDPR compliant consent/explicit consent obtained**	**GDPR compliant consent/explicit consent recorded**
Activity Newsletter Subscription (Mailchimp)	Consent already obtained *Users are required to sign up to the CPGM Newsletter via Mailchimp Website. Users can unsubscribe at any time using the link at the bottom of each newsletter. Completing this step will automatically remove the*	Consent recorded in Mailchimp *(Name filing system/computer)*

	user from the mailing list via Mailchimp.	
WhatsApp Community	Users can opt out at any time by leaving the individual Locality group within the community or the community itself.	WhatsApp

Template G: Tell people about your processes: the Privacy Notice

When you collect personal data from a data subject you must provide the data subject with relevant information; the Privacy Notice. This should be available from CPGM (Privacy notice – Community Pharmacy Greater Manchester), for example, on the CPGM website; and you should draw the attention of new contractors to the Privacy Notice. If you require a copy of the latest Privacy Notice please contact the Services and Contractor Support Lead.

Template H: Ensure data security

The GDPR requires data controllers to take appropriate technical and organisational measures, and adopt appropriate policies, to ensure personal data is processed securely.

Existing measures should be reviewed recognising that some people do seek unauthorised access to personal data. The information available for community pharmacies should be considered and equivalent policies adopted, as appropriate, by LPCs to ensure the physical, electronic and human security of personal data.

You also need to ensure data quality.

Security issues	**Measures**	**Date measures confirmed**
Physical	The following existing policies for LPC's should be considered and adopted as appropriate: Template 6: Asset Register (MS Excel) Template 7: Physical Security Risk Assessment	12/03/2026
Electronic	The following existing policies for LPC's should be considered and adopted as appropriate: Template 8: Mobile Computing Guidelines Template 9: Portable equipment Template 10: Disposal of Portable Assets You must list and carry out a risk assessment for any of your computer systems that do not have an individual log-in and mitigate the risks associated with these systems. The standards of NHS mail are laid out within your user agreement, and further practical considerations are listed at Community Pharmacy England's NHSmail webpage. Learn how to use NHSmail safely, i.e. note that patient data can be communicated securely when both sender and recipient are using an NHSmail account.	12/03/2026

	Fax machines should only be used to send sensitive data as a very last resort and, when used, staff should consider local "Safe Haven" procedures. Fax numbers should be checked and verified before confidential information is sent to them. You can monitor systems and logs for unusual activity that might pre-emptively indicate an attack on your system. Your system supplier or IT department may assist with this. Maintain awareness of cyber risks, e.g. staff should be made aware of the risks from scam, faked or 'phishing' (information-seeking) emails, and be wary of clicking on internet links within emails. Carefully consider the "Ten steps to help improve data and cyber security within your pharmacy" briefing document which includes further information about electronic data security and the extent to which these may apply to CPGM.	
Human	The following existing policies for community pharmacies should be considered and adopted as appropriate: Template 2: Staff Confidentiality Agreement Template 3: Staff Confidentiality Code Template 4: Data Handling Procedure Template 13: Audit Sheet Template 14: Staff Signature List Template 15: Access Control and Password Management Procedure	12/03/2026

LPCs may need to rely on appropriate experts to provide the relevant technical assurances, for example, PharmOutcomes or others providing technical support and ensure you comply with the technical standards required by the NHS.

You should review your data security policies and practices at least annually. Any personal data breaches may result in a review of policies and a review of the incident management procedures.

Template H: Continued

DATA QUALITY

There should also be effective data quality controls in place and the policy could be that only authorised members of staff may add to, amend or delete personal data.

Activity	**CPGM Office team names or groups of staff**
Adding information	Contractor Database: Business Support Team, Communications & Engagement Lead External Database: Business Support Team, Communications & Engagement Lead Confidential HR Files: HR and Finance and Governance Sub Group Lead
Amending information	Contractor Database: Business Support Team, Communications & Engagement Lead External Database: Business Support Team, Communications & Engagement Lead Confidential HR Files: HR and Finance and Governance Sub Group Lead
Deleting information	Contractor Database: Business Support Team, Communications & Engagement Lead External Database: Business Support Team, Communications & Engagement Lead Confidential HR Files: HR and Finance and Governance Sub Group Lead

Template I: Consider personal data breaches

(IG Template 11 updated)

Community Pharmacy Greater Manchester **Information Security Incident Management Procedures**				
Procedures Prepared by: Adrian Kuznicki	Procedures Approved by: Ifti Khan	Date Next Review Due:	February 2026	
Date Prepared: January 2026	Date Approved: 12/03/2026	Date Review Takes Place:	March 2027	

Information security incidents are any event that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, the integrity of the system or data put at risk or the availability of the information through the system being put at risk. Incidents may include theft, misuse or loss of equipment containing confidential information or other incidents that could lead to authorised access to data.

'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 transmitted, stored or otherwise processed.

1. Procedures for dealing with various types of Incident

All CPGM office team should report any suspicious incidents to the Services and Contractor Support Lead and/or CPGM IG Lead Ifti Khan.

Incidents should always be investigated immediately whilst there is still the possibility of collecting as much evidence as possible. Investigations should normally be co-ordinated between at least the Services and Contractor Support Lead & CPGM IG Lead Ifti Khan.

The following procedures should be followed for particular personal data breaches:

A) Theft of equipment holding confidential information and unauthorised access to an area with unsecured confidential information:

- Check the asset register to find out which equipment is missing.
- Investigate whether there has been a legitimate reason for removal of the equipment (such as repair or working away from the usual base).
- If the cause is external inform the police and ask them to investigate.
- If the cause is internal, establish the reason for the theft/ unauthorised access.
- Consider whether there is a future threat to system security and the need to take protective action e.g. change passwords.

B) Inadequate disposal of confidential material (paper, PC hard drive, disks/tapes):
This type of incident is likely to be reported by a member of the public, a patient affected, or a member of staff;

- Investigate how the data came to become inappropriately disposed.
- Take appropriate action to prevent further occurrences (e.g. disciplinary, advice/training, contractual).

C) Loss of data in transit.

- Investigate, as far as possible what has gone missing and where.
- Take appropriate action to prevent further occurrences (e.g. was the envelope correctly addressed, is there further safeguards that could be introduced).

2. Procedures for recording incidents

A record of all incidents, including near-misses, should be made by completing a copy of the information security incident report form (section 3 below).

Incidents should be classified in the log according to the severity of risk to patients and the pharmacy using the following incident classification system described below. For near-misses, consider the likely impact if the breach had occurred.

You must document any personal data breaches, as above, even if they are not notified to the ICO. The ICO may inspect your records to verify you are keeping such records.

Incident or personal data breach classification:

Insignificant: (very low risk)	Minor: (low risk)	Moderate: (Likely to result in a **risk** to the rights and freedoms of patients)	Major: (Consider whether likely to result in a **high risk** to the rights and freedoms of patients)	Critical: (Likely to result in a **high risk** to the rights and freedoms of patients)
Minimal risk - indiscernible effect on stakeholder or CPGM Not reported to ICO	Minor breach, for example data lost but files encrypted, less than 5 stakeholders affected	Moderate breach, for example unencrypted clinical records lost, up to 20 stakeholders affected	Serious breach, for example unencrypted clinical records lost Reported to ICO	Serious breach in terms of volume of records Reported to ICO Communication to data subjects likely

No data subjects informed Recorded as a personal data breach	Not reported to ICO No data subjects informed Recorded as a personal data breach	Reported to ICO Communication to data subjects considered Recorded as a personal data breach	Communication to data subjects considered Recorded as a personal data breach	Recorded as a personal data breach

3. Reporting incidents

Incidents and personal data breaches should be reported to the Services and Contractor Support Lead.

The CPGM IG Lead will determine whether there is also a need to report the incident to others depending on the type and likely consequences of the incident, e.g. inform the ICO, data subjects, Police, NHS England, the LPC insurer (contact CPE for details if relevant) etc.

Notifying the ICO and informing the patient

If the breach is **likely** to result in a risk to the rights and freedoms of a patient, the ICO should be informed of the breach. Notifying the ICO must be done without undue delay, and no later than 72 hours after you first become aware of the breach.

If the breach is likely to result in a **high risk** to the rights and freedoms of a patient, the patient should be informed of the breach. This is subject to certain caveats.

Currently, there is little guidance about the risks to the rights and freedoms of patients, but it is suggested that:

- if personal data is lost in a pharmacy or in a controlled environment, this is unlikely to be a risk to the rights and freedoms of patients.
- if a prescription is lost in a public place, this is likely to be a risk to the rights and freedoms of the patient.
- if there is disclosure of a patient's medical condition to an unauthorised person, this is likely to be a high risk to the rights and freedoms of the patient.

Any notification to the ICO must describe the nature of the breach, such as numbers of data subject, records and what was lost e.g. a prescription; the name and contact details of the DPO; likely consequences of the breach; measures you have taken, for example to mitigate any adverse effect. Where any information is not possible to provide immediately, it may be provided later, but without undue delay.

Template J: Consider personal data breaches (part 2)

(IG Template 12 updated)

Reference number		**Pharmacy/branch name**	

Incident details

Date of incident	
Location of incident	
Summary of incident (State facts only and not opinions. Include details of staff involved and any contributing factors)	
Incident classification (see incident management procedure for guidance)	
Brief description of action already taken	

Actions taken to prevent a reoccurrence			
Has the IG Lead been informed?	Yes ☐	**Has the local NHS England and NHS Improvement team been informed?**	Yes ☐
	No ☐		No ☐
Have you contacted your insurers?	Yes ☐	**Has the Information Commissioner's Office (ICO) been informed?**	Yes ☐
	No ☐		No ☐
Details of any advice provided to pharmacy			

Reporter details

Name		**Job title**	

Information Governance Lead follow up

Investigations, findings and planned actions			
IG Lead Name		**Date**	

Template K: Think about data subject rights

Activity: Consider the following data subject rights you may be asked about.

Right	Details
The right to be informed	Privacy Notice and, as appropriate, bringing the data subjects' attention to the notice. Note requirements if personal data is received from third-parties- the data subject must be informed within a reasonable time (one calendar month) and at least on the first communication. **If the data is pseudonymised and you do not have access to the patient information you do not have to do this.**
The right of access	Provide the information you hold on the data subject free of charge **within one calendar month**, unless you explain why not and possibility of lodging a complaint to the ICO. (Also, potentially other information on processing, but this is usually provided in the Privacy Notice). **Generally, you cannot provide information on request if the data subject is not identified in the data (the data is pseudonymised).**
The right to rectification	For CPGM, the right to rectification – correction – should be straightforward for contractor data and generally will not be applicable to pseudonymised data.
The right to erasure	This may be applicable to contractor personal data (not business data) and generally will not be applicable to pseudonymised data.
The right to restrict processing	For example, while the accuracy of the data is verified by you, or to stop you destroying the record according to CPGM protocols, because the data subject wants you to keep it for the purposes of a legal claim.
The right to data portability	Generally, this right is **not** relevant to CPGM. This right applies only in certain circumstances, for example, if lawful processing of the personal data is by consent of the data subject or a contract and is carried out by automated means.
The right to object	Data subjects have the right to object to you processing their data (in the performance of a task in the public interest) and if they do you will have to consider whether your need to continue processing (e.g. holding a record) overrides their interests, rights and freedoms. In most cases, you will need to retain the data according to your retention policy. The National Data Opt-Out will need to be applied when it is introduced although this is unlikely to apply to CPGM.
'Automated decision -making'	Generally, this right is not relevant to CPGM records.

Template K: Continued

Activity: Keeping a log of data subject rights.

You should also keep a log of those exercising their data subject rights, for example, those asking for a copy of their records, so that you can show you are complying with this part of the GDPR.

DATA SUBJECT RIGHTS – LOG OF REQUESTS			
Name	**Date of request**	**Type of right/request and information provided**	**Date completed**
e.g. Mr P Smith	*1 June*	*right of access – clinical IT system record provided*	*4 June (within one calendar month)*
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

You should seek advice if you receive a data subject request with which you are unfamiliar.

In brief, generally any personal data you collect by consent must be deleted if consent is subsequently withdrawn, with various exceptions including potential legal proceedings.

Template L: Ensure privacy by design and default

The GDPR makes privacy by design – data protection by design and default a legal requirement, indicating that you need to implement technical and organisational measures to ensure you only process personal data necessary for the task, taking into account what you are doing with the data, how long it is being stored, the accessibility required and the risks involved given the nature and scope of the data.

Consider your use of personal data to support CPGM:

Activity	**Issues**	**Date confirmed**
Processing of data to support locally commissioned services	Is patient data pseudonymised?	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

There will be other activities and other examples you can list to ensure that you process data with the minimum risk to patients, the data subjects.

Template M: Data protection impact assessment (DPIA)

Data controllers introducing new technologies or where processing is likely to result in a **high risk** to the 'rights and freedoms of individuals' must carry out a DPIA.

High risk processing includes large-scale processing of special categories of personal data, such as healthcare data, but this is **unlikely to apply to LPCs.** The ICO will be introducing updated guidance on DPIAs soon.

Where appropriate, the views of data subjects, including patients, should be sought.

a DPIA should include consideration of:

- a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing in relation to the purpose;
- an assessment of the risks to individuals;
- the measures in place to address risk, including security and to demonstrate that you comply;
- unmitigated risks (uncontrolled) have been identified and notified to the ICO; and
- a DPIA can address more than one project.

The policies and guidance previously supporting the Data Security and Protection Toolkit (DSPTK) ('Toolkit') are:

Template 1: IG Policy

Template 2: Staff Confidentiality Agreement

Template 3: Staff Confidentiality Code

Template 4: Data Handling Procedure

Template 5: Patient Information Leaflet **(Not relevant policy to CPGM)**

Template 6: Asset Register (MS Excel)

Template 7: Physical Security Risk Assessment

Template 8: Mobile Computing Guidelines

Template 9: Portable equipment

Template 10: Disposal of Portable Assets

Template 11: Incident Management Procedures **(revised version in this booklet)**

Template 12: Information Security Incident Report Form **(revised version in this booklet)**

Template 13: Audit Sheet

Template 14: Staff Signature List

Template 15: Access Control and Password Management Procedure

Template 16: Business Continuity/Emergency Plan

Template 17: Data quality policy

Template 18: Mapping Risk Register

Template 19: Data Flow Mapping

Note: These templates and guidance and the Toolkit may be further updated after the publication of this version of the GDPR WB.

Signed and dated for approval

Adrian Kuznicki

Role – Services and Contractor Support Lead

Date – 12/03/2026

Ifti Khan

Role – CPGM Board Member (IG Lead)

Date – 12/03/2026