DERBY AND DERBYSHIRE LOCAL MEDICAL COMMITTEE (DDLMC) POLICY FOR THE IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

The European statement of GDPR is at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. The GDPR will be encapsulated in UK legislation, one underlying aspect of which is that legislation cannot form a barrier to trade. Note that every country in the European Economic Area which subscribes to the GDPR has the right to make its own, more stringent, regulations. These regulations are yet to be published and we may need to amend this policy if the UK does produce more stringent regulation in due course.

The GDPR applies only to personal data which is **information relating to or identifying** a **living individual**.[1] That identifying information includes the obvious, such as a name or address but could include less obvious data, e.g. an email address (including work e-mail) or electronic mobile phone identity code.

The Information Commissioners Office (ICO) has produced a document '12 steps to take now' and a self-assessment tool to help with preparation for the new regulation. DDLMC needs to maintain security of information about its members, staff members, GPs and other staff at practices and other colleagues. This policy sets out how that intent is to be achieved, both now and in the future, when GDPR is in force from 25th May 2018.

The lead Data Supervisory Authority for DDLMC is the Information Commissioners Office (ICO).

Derby and Derbyshire Local Medical Committee is the Data Controller for the personal data held by DDLMC, Derby and Derbyshire Local Medical Committee Limited and General Practice Task Force (GPTF) Limited.

A Data Protection Officer is not required for DDLMC.

THE INFORMATION

What information is held. See Annex A. Not all of that is Personal Data within the meaning of the GDPR but it is all held in the same places and thus must receive the same levels of protection.

Where the information is held.

> DDLMC Members. Contact information for these people is maintained as electronic files on the Shared Drive, within E-mail address books and may also be held in hard copy files where required. Bank account details are also held which are classified as Personal Information.
>
> DDLMC staff. Contact information for these people is maintained as electronic files on the Shared Drive, within E-mail address books and may also be held in hard copy.

[1] Article 4(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

files where required. Bank account details are also held which are classified as Personal Information.

GPs and other staff at practices and other colleagues. Contact information for these people is maintained as electronic files on the Shared Drive and within E-mail address books.

Why that information is held. There are five main reasons why, under GDPR Article 6(1), a DDLMC can lawfully hold Personal Data. These are: Consent (6(1)(a)), Contract (6(1)(b)), Compliance with Legal Obligation (6(1)(c), Official Authority (6(1)(e) and Legitimate Interest (6(1)(f)).

DDLMC Members. Data could lawfully be held on the basis of Consent, Official Authority and Legitimate Interest. DDLMC relies on Legal Obligation as the lawful basis for processing this data.

DDLMC Staff. Data could lawfully be held on the basis of Consent, Contract, Compliance with Legal Obligation and Legitimate Interest. DDLMC relies on Contract as the lawful basis for processing this data.

GPs and other staff at practices and other colleagues. Data could be lawfully held on the basis of Consent, Compliance with Legal Obligation and Legitimate Interest. DDLMC relies on Legal Obligation as the lawful basis for processing this data.

DEALING WITH THE INFORMATION

Internal processing. Data is held in two main forms:

Hard Copy. Data which is held in hard copy is used for reference when dealing with HR, health and safety, pensions, attendance at courses and other purposes in pursuit of the LMC objectives. It is held securely in locked filing cabinets which are only accessible by the Office Manager and Chief Operating Officer. If other people require access to this data it will be done under close supervision of the Chief Operating Office.

Electronic data. Most personal data is held electronically on the DDLMC computer system. Data is held on the DDLMC Server which is stored on site at the LMC Office. The Server and associated IT systems are maintained and run by ArdenGEM CSU and benefit from the same protection as other NHS systems. This includes but is not limited to, password protection on all devices, NHS smartcard access for remote laptops, servers held in secure locations, systems regularly backed up, regular security patch and virus software updates. The data is used to contact all parties with an interest in general practice for the purposes of carrying out the aims and objectives of the DDLMC.

Data Sharing. In fulfilling its legal obligation in pursuit of its objectives, including GP representation DDLMC may need to share data with other organisations, including but not limited to BMA (including GPC), RCGP, NHSE and CCGs. On that basis DDLMC will obtain consent to sgare data with these other organisations.

THREATS TO SECURITY AND HOW TO COUNTER THEM

Threats to data security are manifold but mainly break into two categories: technical and physical. The technical threats are those affecting the electronic systems holding the data, such as hacking through the lack of firewalls, unlimited access for company personnel, lack

of data encryption and weak, inadequate or unchanging passwords or even no passwords at all. Much greater threats traditionally are the lack of the physical protection measures to secure the technical systems. If any data can be sent unencrypted then that could be a security breach. If a laptop or phone is unprotected by encryption and passwords and not physically protected from theft or loss then that too could be a security breach. If there is a disaffected or careless member of staff able to access and copy personal data then that could be a security breach. More detail of threats and countermeasures can be found at Annex C.

DATA SUBJECT RIGHTS[2]

All Data Subjects under the GDPR have the following rights, which DDLMC must respect and enable:

The right to be **informed**. This policy explains how DDLMC meet their obligations to inform data subjects about the data that is held on them and how it is processed.

The right of **access**. All data subjects are able to request access to the data that DDLMC holds on them. This will routinely be provided free of charge and any requests received via electronic means will be responded to electronically.

The right to **rectification**. If any data subject informs us that information held by DDLMC is inaccurate then we will investigate and if appropriate correct the data and inform the data subject of the changes.

The right to **erasure**. Data will only be held for a reasonable period of time and in accordance with other legislative requirements, such as financial data. DDLMC will

[2] Article 13. Para1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: *[Para 4 states unless the data subject already has this information]*

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Para 2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

undertake an annual audit of data to ensure it is not holding unnecessary out of date data.

The right to **restrict processing**[3]. DDLMC will obtain consent to process data for reasons other than normal agreed processing.

The right to **data portability**. This is a new right under GDPR. It applies only to personal data provided with the individual's consent or for the performance of a contract and when processing is carried out by automated means. The requirement is that the data be provided, if required, in a structure commonly used and in machine-readable form. This will generally not apply to data held by DDLMC.

The right to **object**. Any data subject may object to DDLMC holding data about them that they consider unnecessary and they have the right to object to it being held and (see above) have the right to have it erased. If there is a legal obligation for the DDLMC to hold this data then DDLMC will inform the data subject.

The right **not to be subject to automated decision-making including profiling.** In the unlikely event that DDLMC intends to carry out any automated decision-making, including profiling, then the data subjects will be:

(1) Warned of the intention
(2) Reminded of their right to restrict DDLMC use of their data for processing

SUBJECT ACCESS REQUESTS

Under GDPR:

DDLMC cannot routinely charge for replying to any subject access request. Replies must be sent within one month. If a request is either manifestly unfounded or excessive[4] DDLMC may either charge a reasonable fee or refuse the request. If refused DDLMC must state why and notify the data subject that they have the right to complain to the supervisory authority.

PERSONAL DATA BREACH POLICY

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. They must do this within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, they must also inform those individuals without undue delay. They must also keep a record of any personal data breaches, regardless of whether they are required to notify.

What is a personal data breach?

[3] Article 13. Para 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. *[See previous footnote]*

[4] Article 12. Para 5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
(b) refuse to act on the request.
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

A personal data breach is defined as 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. 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.

Types of personal data breaches

There are three main categories of personal data breach, which include:

1. Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data
2. Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data; and
3. Integrity breach - where there is an unauthorised or accidental alteration of personal data

Examples of personal data breaches

Some examples of personal data breaches may include (but are not limited to); access by an unauthorised third party; deliberate or accidental action (or inaction) by a controller or processor; sending personal data to an incorrect recipient; computing devices containing personal data being lost or stolen; alteration, deletion or destruction of personal data without permission; and loss of availability or control of personal data.

Reporting Process

The DDLMC will establish whether a personal data breach has taken place and promptly take steps to address it. This will include a decision-making process to report the incident to the Information Commissioner if required.

When a personal data breach has occurred, the DDLMC will:

1. Minimise the impact of the breach by containing it by implementing any actions deemed appropriate
2. Undertake a risk assessment to determine whether the incident requires onward reporting to either the Information Commissioner or to the data subject affected (or both)
3. Ensure recording of all personal data breaches regardless of whether the breach requires onward reporting

Personal Data Breach Identification & Recording

The DDLMC has set up systems and processes to identify whether a breach has taken place, as well as to assess the significance of the risk. In addition, a system to monitor any breaches has also been developed which are in line with GDPR requirements.

Flow Chart & Risk Assessment

The DDLMC will use the Personal Data Breach flowchart in Annex E in conjunction with the Risk to Right and Freedom Risk Assessment in Annex F to identify whether onward notification needs to be made as a result of the breach. In addition, a record of the data breach will be kept in line with monitoring requirements.

The completed template will be completed and returned to the DDLMC Chief Operating Officer (or other nominated executive in his absence) within I working day of the of the incident occurring. The primary focus will be to establish the type of incident and to quickly contain the breach and prevent further adverse effects upon the personal data. It will also allow onward reporting within 72 hours if required. If the breach is financial in nature then the Treasurer is also to be informed within 1 working day.

The risk assessment identifies the likelihood and level of risk that the rights and freedoms of an individual have been affected by the breach. These are highlighted in Recital 75 of GDPR.

Monitoring template

The monitoring template has been designed to ensure all personal data breaches are investigated and measures put into place to address and to mitigate the breach. The excel spreadsheet will be completed to ensure a contemporary record of any incidents to learning can be applied and systems and processes improved.

The monitoring template includes a self-populating Excel spreadsheet:

- Date of the incident
- Date reported to the DDLMC Manager/IG Manager
- Whether a Personal Data Breach has occurred
- Type of Personal Data Breach
- Type of Data Subject
- Type of Data Record
- Number of subjects affected
- Full description of the incident
- Assessment of risk to individual rights and freedoms
- Likelihood of risk
- Risk level
- Severity of risk
- Damage as a result of breach
- Consequence of breach
- Measures taken to address and mitigate breach
- Assessment of whether ICO and Patient need to be notified

Outcome of risk assessment

The DDLMC will ensure that all breaches are recorded, regardless of whether or not they need to be reported to the ICO or the Patient as per the arrangements set out under GDPR:

- No Risk to Rights and Freedoms – the breach does not need to be notified to the ICO
- Risk to Rights and Freedoms – the breach needs to be reported to the ICO
- High Risk to Rights and Freedoms – the breach needs to be reported to the patient

To report the breach, the DDLMC Chief Operating Officer will contact the Information Commissioners Office on the Personal Data Breach helpline on 0303 123 1113 or will complete the online form at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ and send it to casework@ico.org.uk.

The DDLMC will report the breach without undue delay and not later than 72 hours after becoming aware of the breach. If the breach is reported later than 72 hours then it shall be done so accompanied by reasons for the delay. If a breach has been identified, but there is insufficient or incomplete information, the DDLMC will report as much information as is

available at that time to the ICO. Further information will be reported to the ICO as it becomes available.

Data Processors

In the event that The DDLMC uses other data processors and that processor suffers a breach, then under Article 33(2) it must inform the DDLMC without undue delay as soon as it becomes aware. The processor must comply with any investigation, reporting and remedial actions undertaken or determined by the DDLMC.

Informing Data Subjects

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the DDLMC will inform those concerned directly and without undue delay. In other words, this should take place *as soon as possible*.

Whilst the threshold for informing individuals is higher than for notifying the ICO, the DDLMC will inform data subjects potentially affected if the breach was classified as reportable to the ICO.

The DDLMC will describe to individuals, in clear and plain language:

- the nature of the personal data breach
- the name and contact details of our contact point where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects

The DDLMC will not need to inform data subjects if:

a) the DDLMC *had* implemented appropriate technical and organisational protection measures, and those measures *were applied* to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; and

b) the DDLMC *had* taken *subsequent* measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise

The DDLMC will, however, need to inform data subjects *if the ICO*, having been alerted by the DDLMC's notification, and on reviewing the report, decides that data subjects ought to be informed.

Post breach discussion

The DDLMC will investigate the root cause of the breach and identify how a recurrence can be prevented. Any breaches and all subsequent actions will be discussed at the next DDLMC executive/Senior Team meeting.

DATA PROTECTION IMPACT ASSESSMENT AND DATA PROTECTION BY DESIGN

It has always been good DDLMC to adopt a 'privacy by design' approach and to carry out a privacy impact assessment. GDPR makes privacy by design an express legal requirement. Under GDPR PIAs are referred to as 'Data Protection Impact Assessments' (DPIA).

Formally the first step is always to assess carefully whether the organisation needs a DPIA. The assessment at Annex D indicates that while we do not need a DPIA, it is good practice to have a DPIA and this can be found at Annex D.

Annexes:

A. Information held
B. Consent Form
C. Threats to data security
D. Data Protection Impact Assessment
E. Personal Data Breach Flowchart
F. Risk to Right and Freedom Risk Assessment

ANNEX A

INFORMATION HELD

GDPR only applies to personal information, which is defined in Article 4(1) as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

DDLMC Members and Staff. We may hold data such as the following – the list is not exhaustive:

- Title
- First name
- Middle name(s)
- Initials
- Last Name
- Full address including postcode
- Email address(es)
- Home phone number
- Work number
- Mobile number
- Bank Account details
- Date of joining
- National Insurance number

GPs and staff at practices/Other colleagues. We may hold data such as the following – the list is not exhaustive:

- Title
- First name
- Last Name
- Full address including postcode
- Email address(es)
- Home phone number
- Work number
- Mobile number
- Role

ANNEX B

LMC MEMBER/MEMBER OF STAFF CONSENT FORM

I,
of <*address*>
being an LMC Member * / Employee* of Derby and Derbyshire Local Medical Committee and the associated Limited Company hereby agree to DDLMC holding my personal information as data on the understanding that after a period of no greater than 2 years from my ceasing to be a an LMC Member * / Employee* of the LMC, but of seven (7) years in the case of financial data, my personal data shall be deleted from all records unless my specific consent is sought to retain them, such consent not to be unreasonably withheld. In this connection, if any of my personal data shall have appeared in printed material I recognise that I cannot require a retrospective change to that printed material.

Signed:
Dated:

*[*delete what is inapplicable.]*

ANNEX D

THREATS TO DATA SECURITY

<table>
<tr><th>Ser</th><th>Threat</th><th>Counter-measures</th><th>Remarks</th></tr>
<tr><td>1</td><td>Outside technical attack resulting in theft of information</td><td>• Firewalls and virus checkers
• Automated logging of access to the system (Read-only)</td><td>Provided by ArdenGEM</td></tr>
<tr><td>2</td><td>Outside physical attack – theft, loss, burglary</td><td>• Physical security measures
• Passwords</td><td></td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">Unauthorised access</td><td>• Limit the number of people with access to more sensitive personal data
• Automated logging of access to the system (Read-only)</td><td>Currently the only people allowed access to the data are:<table><tr><th>Appointment</th><th>Permissions</th></tr><tr><td>COO</td><td>All</td></tr><tr><td>PA</td><td>All</td></tr><tr><td>CEO</td><td>All</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td>• Strong passwords</td><td>At least 8 digits with a mix of capitals, numerals and special characters</td></tr>
<tr><td>• Passwords to be changed regularly and frequently</td><td>• Changed at least every 3 months and also whenever a new member of staff takes over any one of the posts entitled to access</td></tr>
<tr><td>4</td><td>Unauthorised release</td><td>No information to be given to a third party without the active consent of the data subject</td><td>• Internal disciplinary penalties for breaching that counter-measure must be severe</td></tr>
<tr><td>5</td><td>Sharing to another organisation that fails to protect the information</td><td>Undertakings to be given by the recipient organisation, enforceable by contract, and containing indemnity clauses that data will be:
• Protected to the same standard as by the DDLMC
• Used only for the purpose for which it is released
• Deleted once used</td><td></td></tr>
<tr><td>6</td><td>System failure leading to loss of data</td><td>Regular back-ups, on and off-site</td><td>All done automatically through ArdenGEM</td></tr>
<tr><td>7</td><td>Disaffected Member or Employee with</td><td>Minimise “Write” and “Delete” access to the</td><td></td></tr>
</table>

Ser	Threat	Counter-measures	Remarks
	authorised access	database	
8	Loss of computing power	• Regular back-ups, on and off-site. • Fall-back manual processes	

ANNEX D

DATA PRIVACY IMPACT ASSESSMENT

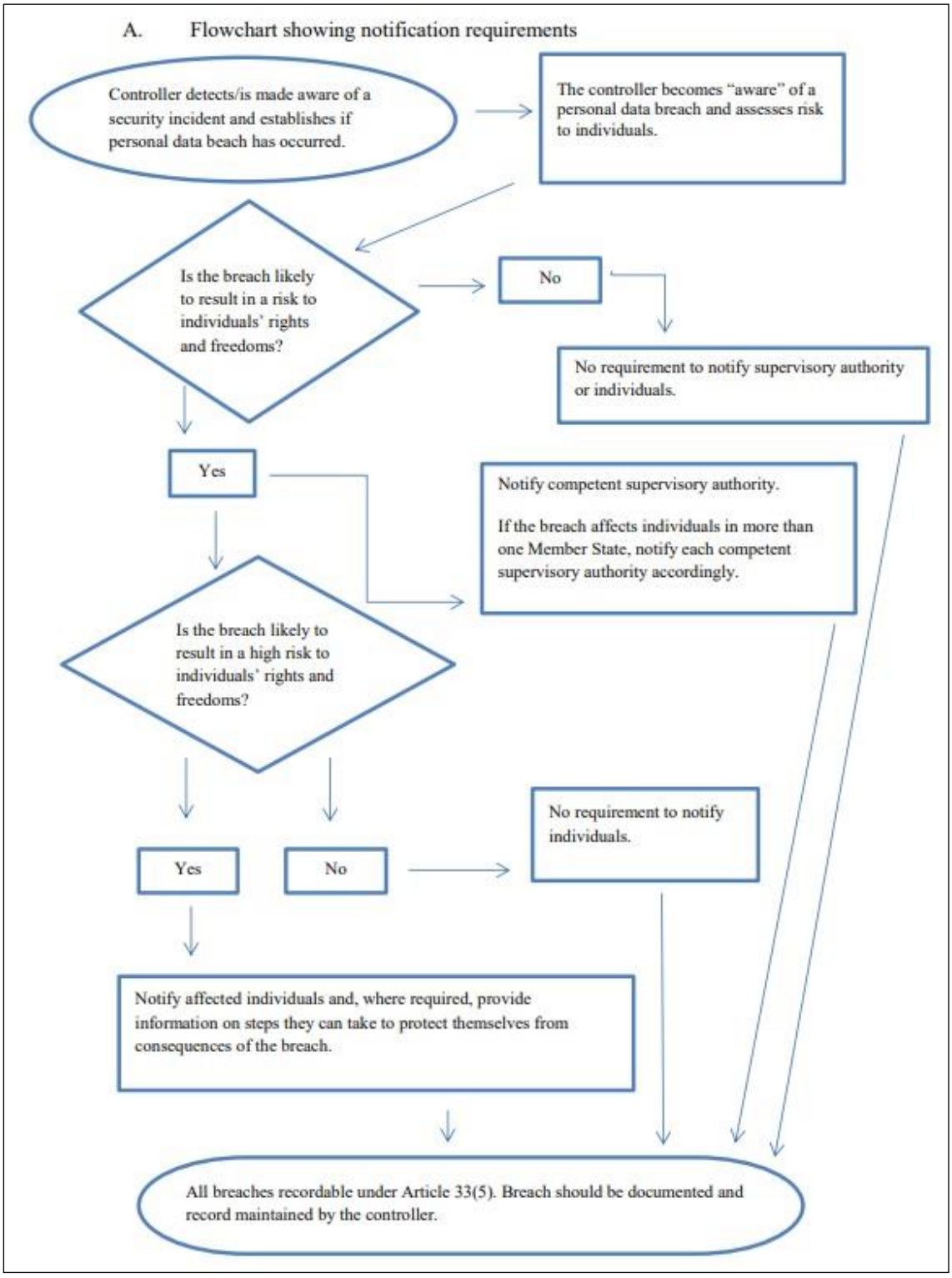
1. Do we need one? This is the first step, and if the answer is 'No' then no further action is needed.

Recommended questions	Suggested Answer for DDLMC
Will the project involve the collection of new information about individuals?	No. The same information as usual will be required in the case of new contacts. Existing contacts will not need to give us new information
Will the project compel individuals to provide information about them?	No. If they choose to join the LMC as Members or staff then they are required to provide certain information
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Only if individuals consent and this will be restricted to things such as work e-mail addresses with BMA/GPC etc
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	Only in the context of employment or membership of the LMC or of any working groups
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	Ordinarily No. There may be rare occasions when data processing raises privacy concerns (e.g. when supporting someone who could potentially be liable to significant professional sanction) but additional data protection procedures are in place for such cases
Will the project require you to contact individuals in ways which they may find intrusive?	No

2. On that basis, we do not need a Privacy Impact Statement.

ANNEX E

A. Flowchart showing notification requirements



ANNEX F

Risk to Right and Freedom Risk Assessment

Risk to Right & Freedom	**Likelihood score**	**Severity Score**	**Outcome**
Discrimination			
Identity theft or fraud			
Financial loss			
Damage to the reputation			
Loss of confidentiality			
Unauthorised reversal of pseudonymisation			
Any significant economic or social disadvantage			
Deprivation of rights and freedoms			
Prevention from exercising control over their personal data			
Reveals racial or ethnic origin			
Reveals political opinions			
Reveals religious or philosophical beliefs			
Reveals trade union membership			
Processing of genetic data			
Data concerning health			
Data concerning sex life			
Data concerning criminal convictions and offences			
Performance at work			
Economic situation			
Health, personal preferences or interests			
Reliability or behaviour			
Location or movements			
In creating or using personal profiles			
personal data of vulnerable natural persons (in particular children)			
Affecting large amount of personal data and affects a large number of data subjects.			

Risk Assessment Matrix

		Likelihood				
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Risk Level	**Catastrophic**	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5

Colour	**Risk level**	**Outcome**
Green	No Risk	Do not report
Amber	Risk	Report to ICO
Red	High Risk	Report to Data Subject