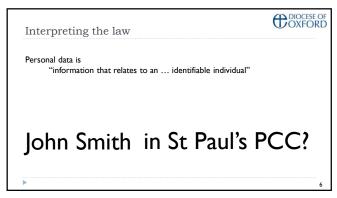




G	DPR: where is your parish/benefice/deanery?
1.	Not started yet
2.	At the planning stage
3.	Some steps taken (for example, Privacy Notice published)
4.	Most areas of parish activity are GDPR compliant
5.	All areas are GDPR compliant
<b>&gt;</b>	



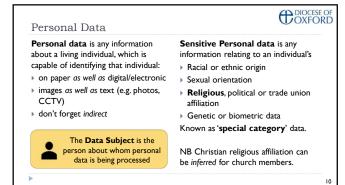


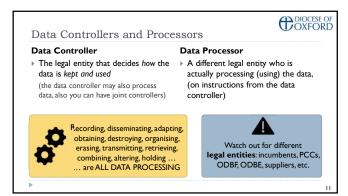






# General Data Protection Regulation (GDPR) Data Protection is about avoiding harm to individuals by misusing or mismanaging their personal data. GDPR is: 1. An extension/tightening of existing data protection legislation (DPA 1998) 2. UK data protection law is now a combination of: EU General Data Protection Regulation 2016/679 (the "GDPR") UK Data Protection Act 2018 (the "DPA 2018") All generally referred to as "GDPR".

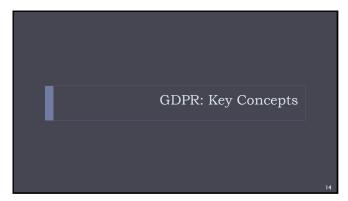






### COXFORD Typical steps for parishes/deaneries: . Raise awareness 9. Update Policies & Privacy Notices Conduct a Data Audit (and data Work out how you will deal with Subject Access Requests mapping) Identify (and document) your 'lawful bases' Data breaches: how will you detect, report and investigate? Check your processes meet the 'eight rights' and 'seven principles' 12. Training 13. Build-in data protection to your Review how you get consent new initiatives Build in extra protection for children Data retention and disposal rochester diocese gdpr toolkit (simpler version at parishresources.org.uk/gdpr) Review your Data Sharing

13



14

### DIOCESE OF OXFORD GDPR: Eight Rights of Individuals Right to restrict/suppress processing In certain circumstances: store data but not use it. ▶ Right to be Informed Informed about the collection and use of their personal data (transparency) Right to Data Portability Right of Access (a.k.a. Subject Access Request) may be made verbally or in writing. One month to respond. No fee. Ease of movement between IT environments Right to Object Absolute right with regard to direct Right to rectification Correcting inaccurate data marketing Rights in relation to automated decision-making and profiling ▶ Right to erasure (right to be forgotten)

<ol> <li>Data processing must be lawful, fair and transparent</li> </ol>	5. Keep data for no longer than necessary (storage limitation),
<ol><li>For explicit legitimate limited purposes only</li></ol>	after which destroy, delete or return it
3. Hold no more data than necessary for the purpose (data minimisation)	<ol> <li>Keep data secure: protect against accidental loss, damage, disclosure (integrity and confidentiality)</li> </ol>
Data must be kept <b>accurate</b> and up to date	<ol> <li>Data controllers are accountable for compliance and must be able to demonstrate compliance</li> </ol>

## Six Lawful Bases for holding/processing data 1. Legitimate interest – needed for performance of main business, and 'balance of interests' 2. Necessary to fulfil contractual obligation 3. Legal obligation of the data controller 4. Data subject has given consent 5. Needed to protect vital interests (i.e. someone's life) of the data subject 6. Public task For each type of data: decide which lawful basis is most appropriate for holding/processing that data. Get it right first time – there are implications!

Typical Parish Data: lawfu	ul bases (suggested)
Legitimate interest	Contractual obligation
Parish office holders: PCC etc.	► Employees
▶ Rota members (may be consent?)	Legal obligation
Consent	▶ Pre wedding identity checks
► Membership	Electoral Roll
Parish magazine / email (publicity)	Giving (Gift Aid)
	<ul> <li>Registers (baptisms, marriages)</li> </ul>
<b>&gt;</b>	

Other Requirements you sl	hould be aware of
Data storage Data must be stored within the European Economic Area or, if stored outside, to standards equivalent to GDPR (e.g. Privacy Shield in USA)	Subject Access Request  Request for copy of data held  No charge, one calendar month to respond
<b>Data sharing</b> Data controller's responsibility to control/restrict the use of data shared with other organisations (data sharing agreement).	Risk Management  Encourage the reporting of Data Breaches: record and react  Data Processing Impact Assessment (DPIA) for high risk activity (unlikely)

## Registering with the ICO?

- Data controllers may need to register with the Information Commissioner's Office
- Many charities and not-for-profit organisations are exempt from registering ... and therefore do not need to pay a fee.
- However ... if you use CCTV for the purposes of crime prevention, registration is mandatory

If you do have to register, and pay a fee, charities and not-for-profit organisations pay a Tier I fee of £40/year

DIOCESE OF OXFORD

## Self assessment:

- ico register self assess
- ico how much will i need to pay

20

## Useful Sources of Information

- Diocesan website: www.oxford.anglican.org/ (under Support Services, GDPR)
- ICO Guide to GDPR: ico.org.uk (under General Data Protection Regulation (GDPR))



21

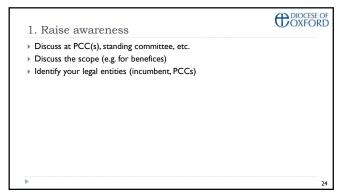
DIOCESE OF OXFORD

GDPR: Journey to Compliance

22

### DIOCESE OF OXFORD Typical steps for parishes/deaneries: 9. Update Policies & Privacy Notices . Raise awareness 10. Work out how you will deal with Subject Access Requests 2. Conduct a Data Audit (and data mapping) Data breaches: how will you detect, report and investigate? Identify (and document) your 'lawful bases' Check your processes meet the 'eight rights' and 'seven principles' 12. Training 13. Build-in data protection to your 5. Review how you get consent new initiatives Build in extra protection for children Data retention and disposal rochester diocese gdpr toolkit (simpler version at parishresources.org.uk/gdpr) Review your Data Sharing

23



Data	audit:		Data mapping (optional next step):					
	all the places wh sonal data and w			s you s cal 'chu	ort the	differ	ent dat	a into
Du	ta Protection Audit							
	Year care Name of data (springer)							
	Charles and administration of the control of the co						200	
1.	Appeal Securing gast nuclear production	Data Mapping Document					(I	OXFOR
1		Data Mapping Document  Church House Oxford: Overty	pe Teamy/Dept Name	t Hierer			(I	POXFOR
1	What personal sizes are you knowing		Collection Fund the Where does the	Processing Auditholians What are you thing with K, and why (out. Tauful hand)	Cutations, Localities & Access Strate, where, who can extract & felow magnifered. Second?	Data Maring? If so, with which other legal armbes	Retention Policy How long to tens, How applied?	OXFOR
8	What details the pass tensor?	Church House Culord: Overty Reson What are you trang What load of a to do 8 why?	Collection Point stal Where does the data come found	Proceeding Audithoritors What are you thing with X, and only (both TauAul Basis) French or the security of develop-become on the Committee of the Security Security of the Security Sec	& Recent what, where, who can some & how moretained. Secure?  1) Files on desire E. and E. dere Exert specifies. 1) Page files	For, with which	Contact details debted to come to the get successive that an extension that an extension that	Impart UM/In Likelihood: UM
1	Minut personal data on you benging	Church House Caford: Overty Resease (Most a Gregoria (Most as see form) (Most as see form	Collection front of Where dues the data come from?	Processing Auditivation What are pro-dring with it, and why (not. lawful base) Funded to alread amounts of contents	& Access What, where, who can screen & felow montproved. Secure? 1; Film in Making NC, and R. done (Secure)	Fig. with which other legal articles Subsept offices of Donness Regions	Contact details debted as you as the per architecture field	Impart 1/M/M Chellhood 1/M Imper 3/ Litelbook M

Legitimate int			
Contractual o	bligation		
Legal obligation	n		
Consent			
Vital interests			
Public task			
ide, in each ca	se, which one is mo	st appropriate.	

Right to be informed (transparency)	1. Processing: lawful, fair and transparent
Right of access	2. For explicit and legitimate (limited)
Right to rectification	purposes only
Right to erasure	3. Using the minimal data necessary
Right to restrict/suppress processing	4. Kept accurate and up to date
Right to data portability	5. Kept for no longer than necessary
. Right to object	Kept safe from corruption or
Right in relation to automated	unauthorised access
decision-making and profiling	7. Data controllers: accountable and able to demonstrate compliance

5. Review how you get consent	
Decide when consent is needed (part of your 'lawful basis' decision)	
Giving consent:	
Dpt-in and Opt-out: equally straightforward	
Cannot default to Opt-in	
<ul> <li>"Granularity": multiple Opt-ins must be separate, not linked</li> <li>Must be freely given</li> </ul>	
Influst be freely given     Unambiguous	
Use age-appropriate language	
Consent must be recorded for future reference	
Withdrawing consent – must also be recorded!	
	-
28	
28	
DIOCESE OF OXFORD	
6. Build in extra protection for children	
▶ Children's personal data merits specific protection (due to increased risks)	
▶ Be clear about	
where a child is the data subject	
who gives consent for you to process data about a child?	
<ul> <li>Any privacy notice or consent statement intended to be read by children must be in plain, age-appropriate, language</li> </ul>	
Consult with children when designing processing of their data?	
Consent: no set age at which children are considered competent to provide their own consent to processing (under GDPR, 13 year-olds capable of giving	

7. Data retention and disposal	DIOCESE OF OXFORD
How long do you need to keep the data?	
When do you stop using it?	
Do you need to archive it?	
Records kept for safeguarding purposes?	
▶ How you delete/dispose of it?	
Deletion of electronic records	
Regular (annual?) reviews of data e.g. of contacts in email/mobile phone	
church of england records management	
"Keep or Bin? The Care of Your Parish Records"	
<b>&gt;</b>	30

<b>△</b> DIO	CESE OF
8. Review your Data Sharing	FORD
<ul> <li>Find out which legal entities you share data with</li> <li>Who is the data controller and who is the processor?</li> </ul>	
Examine the agreement you have with them from a data perspective     Does the agreement specify what data is shared and what the other party can and	
cannot do with the data	
<ul> <li>Look for commitments that they do not share the data further</li> <li>Ask them: are they GDPR compliant?</li> </ul>	
<ul> <li>Beware of taking 'yes' for an answer – probe, check their website</li> <li>Ask for a formal letter confirming that they comply (and will inform you if they cea</li> </ul>	use
to comply)  Do you need further work: contract amendment, data sharing agreement?	
▶ Prioritise the higher-risk organisations	
<b>&gt;</b>	31
31	
(A) DIO	CEST OF
9. Update Policies & Privacy Notices	FORD
Sample privacy notice:     \begin{align*}     \begin{align*}	
Beware of copying other peoples' mistakes	
<b>&gt;</b>	32
32	
32	
10. Subject Access Requests	FORD
Unlikely, but could be contentious if it happens	
At least have an outline plan of how you would handle a SAR	
<b>.</b>	33
22	
33	

	DIOCESE OF OXFORD		
11. Data breaches	OATORD		
<ul> <li>Be aware of the possibility of a data breach</li> <li>Likely risk areas:</li> </ul>			
Loss/theft of data (e.g. laptop, phone or tablet stolen)			
<ul> <li>Email or social media account hacked</li> <li>CVs or other sensitive/confidential documents disclosed</li> </ul>			
<ul> <li>How will you detect, report and investigate?</li> </ul>			
		•	
<b>•</b>	34		
34			
40 5 1	DIOCESE OF OXFORD		
12. Training			
What additional awareness or skills might be required?			
<b>-</b>			
-	35		
5			
13. Build-in data protection to your new initi	DIOCESE OF OXFORD		
13. Build-in data protection to your new initi	latives		
<ul> <li>'Privacy by design': you make data protection considerations whe new activities and areas of involvement</li> </ul>	en mu oducing		
Risk assess new activity (DPIAs) watch out for:			
<ul> <li>Linked databases</li> <li>Vulnerable data subjects (elderly, children, those who are unwell)</li> </ul>			
► New technologies			
MATERIAL PROPERTY.			