What does GDPR mean for BATOD?

Data Breaches

A breach – is the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The above can cover anything, from the loss of a laptop, email addresses being shared in error - often using the to: or cc: field - to confidential information sent to the wrong address or access to systems that a BATOD member has no right to access. It is worth knowing that until breaches are confirmed they are often referred to as data protection incidents.

If you suspect a breach has occurred you must contact the BATOD data protection officer (DPO) email: **dpo@batod.org.uk**

If any of these occur then the greatest loss to BATOD will be reputation and trust.

The sooner the DPO is aware of an issue, the sooner steps can be taken to limit the amount of damage that a breach could cause.

Where data breaches have the potential to cause a high risk or damage to the individuals affected, they need to be contacted to make them aware of the potential risk. If action can be taken to help the people affected it should be taken immediately.

Not following processes leaves BATOD open to the risk of fines, for both non-reporting of the breach and for the breach itself.

Remember to always follow these steps:

- Report
- act to protect those affected
- investigate and record

- learn from mistakes.

The most significant change under GDPR is that BATOD must report certain breaches to the Information Commissioner's Office (ICO) within 72 hours. This 72 hour window starts when a BATOD officer is made aware of an incident, not when the BATOD data protection officer is made aware. Breaches must therefore be notified to the BATOD DPO and the BATOD President immediately and certainly within 24 hours.

Breach Notification - Breach notifications are now mandatory and this notification is expected to be made within 72 hours of the breach occurring. The reporting method for any breach will need to be understood by all BATOD officers and breaches reported as soon as possible.

Sanctions - Previously, under the DPA, the maximum fine that could be issued was £500,000. This will increase to 4% of annual revenue or €20m.

New Rights - Under GDPR, people have enhanced and new rights. Notably it will be easier to access the information an organisation holds on them. There is a right to be forgotten.

Responsibilities - BATOD officers have a responsibility to ensure that

- they follow the law, and the rules laid down by BATOD
- their actions are honest
- security is an integral part of their duties.

Information Asset Register - BATOD needs to know the information that officers hold therefore officers holding sensitive information will be required to complete an Information Asset Register by 30 September of each calendar year.

Penalties

The ICO issued fines of £3.2 million during 2016, making the UK one of the most fined countries in Europe.

Under the GDPR, fines will rise from £500,000 up to €20,000,000 or 4% of global turnover.

The likelihood of compensation claims will also increase as people have the right to bring claims for immaterial damage.

- BATOD must develop and maintain retention inventories of all important information assets.
- It is the responsibility of every individual to ensure that the information they manage or process is kept in accordance with this guidance

Hard copies of sensitive information (e.g. names and addresses)

Paper copies must not be produced or kept. All historic hard copies should be disposed of securely e.g. using a fine cross cut shredder

Passwords

- Keep your passwords to yourself
- Avoid guessable passwords
- Change your password if you think it's been compromised

PCs and laptops

Laptops handling BATOD data should be encrypted and password protected

- Never let anyone else use your logon details
- Steps should be taken to ensure unauthorised persons cannot access/view BATOD sensitive information
- Lock your workstation (using the Ctl-Alt-Del keys) when leaving your desk

- Switch off if you're away from your device

- Laptops should be securely transported and stored. They should not be left in a vehicle overnight and should not be left in view in a car during the day time

- Personal iCloud storage should not be used

Emails

Saved emails from former members should be deleted to ensure that their personal data is no longer held. Personal or sensitive information must not be sent by email. If access to such information is required, then members should contact the NEO/ Assistant NEO who can give temporary access to such information via the BATOD cloud.

Removable media devices

- All data stored on removable media devices **must** be encrypted. Removable media devices such as USB memory sticks must only be used to transfer information from device to device and the data should be erased immediately. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they take reasonable care to avoid damage or loss.
- Damaged or faulty removable media devices must not be used.
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data loss.

Backing up data

All BATOD data should be backed up to the BATOD Cloud.

Retention policy

BATOD will keep information for the following periods:

Information	Timescale	Where
Minutes of BATOD meetings	Long term	Website
Correspondence relating to decisions	Long term	On BATOD cloud
General correspondence	Long term	On BATOD hardware and secure Gmail
Financial information August - July	8 financial years or 6 financial years after officer leaves BATOD	On BATOD cloud
Tax information	8 financial years or 6 financial years after officer leaves BATOD	On BATOD cloud & Treasurer's PC
Payroll information	6 financial years after officer leaves BATOD	On BATOD Cloud & Treasurer's PC
Bank statements Accounts.	8 financial years	Annual report and then saved on BATOD cloud On BATOD cloud also on the annual report which is placed on website
Members personal details	Deleted on leaving BATOD	On BATOD cloud
Committee paperwork	Long term - archived every 2 years	On BATOD cloud
Consultant requests	Archived annually	On BATOD cloud
Registers of attendance at training days, events, AGMs, regional and national meetings	Deleted after the event	On regional committee members' hardware backed up to personal cloud

Website www.batod.org.uk
Email batod_aneo@icloud.com
Telephone 07506 400280

Teresa Quail
National Executive Officer

Con Powell applications	Deleted if not successful by 30 September annually. For successful applicants for 7 financial years post qualifying	On BATOD cloud
CRIDE tracking sheet	Deleted when used	On BATOD cloud
Journal and magazine address data	4 months	On BATOD cloud
Images and videos for use in BATOD publications	Three years **but consent can be withdrawn at any time**	On BATOD website and BATOD cloud

No BATOD information is allowed to be sold or given to anyone else.

Photos and video recording at BATOD events

All participants at BATOD events should be informed prior to any photos or media recordings being taken**.** They should be informed where these photos or recordings may be used.

It is expected that all BATOD officers read and comply with all procedures contained within this document.

I have read, understand and agree to follow the guidance contained within this document.

I understand that if I am unsure about any of this guidance that it is my personal responsibility to seek clarification from the BATOD DPO email: **dpo@batod.org.uk**

PRINT NAME _____

SIGNATURE _____

Role within BATOD _____

DATE _____

➢ Please keep hold of this document for your information and reference.

- If you wish to discuss any points raised in this document please contact the BATOD DPO
- If you require this information in another format please contact the DPO
- Available in BSL on request

Website www.batod.org.uk
Email batod_aneo@icloud.com
Telephone 07506 400280

Teresa Quail
National Executive Officer