South Wales
Fire and Rescue Service

Gwasanaeth Tân ac Achub
De Cymru

DATE:	12 July 2018	FOI REQUEST NO:	036_1819

FOI REQUEST AND RESPONSE

I am writing to make a request for information under the Freedom of Information Act 2000.

1. **Have you invested in technology specifically to comply with GDPR?**
   No investment has been made specifically to comply with GDPR. Our Data Protection Officer has worked alongside ICT for many years and the protection of personal data has always been a part of the overall ICT strategy.

2. **Which information security framework(s) have you implemented?**

   National Procurement Service Information Assurance Services framework

3. **Have you signed contractual assurances from all the third-party organisations you work with requiring that they achieve GDPR compliance by 25 May 2018?**

   The data protection office is reviewing all agreements and, where appropriate, these are being updated in line with the requirements of the GDPR. This includes contract documents, as well as MOU's and Information Sharing Protocols. However, the protection of personal data has always been a part of this work, in line with the Data Protection Act 1998.

4. **Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?**
   - YES

5. **Do you use encryption to protect all PII repositories within your organisation?**
   All our electronic systems are protected by a wide range of security methods, regardless of the type of data stored within them. Encryption is in place where appropriate.

6. **As part of this audit, did you clarify if PII data is being stored on, and/or accessed by:**
    a. Mobile devices
    b. Cloud services
    c. Third party contractors

    YES

7. **Does the organisation employ controls that will prevent an unknown device accessing PII repositories?**
    - Please refer to question 5
    -
8. **Does your organisation employ controls that detect the security posture of a device before granting access to network resources – i.e. valid certificates, patched, AV protected, etc.**
    - Please refer to question 5

9. **Should PII data be compromised, have you defined a process so you can notify the relevant supervisory authority within 72 hours?**
    - Yes

10. **Have you ever paid a ransom demand to have data returned / malware (aka ransomware) removed from systems?**
    SWFRS have and will continue follow the latest guidance from the National Cyber Security Centre (NCSC) and National Crime Agency (NCA) in all aspects of organisational security and in particular the payment of Ransomware

11. **To which positions/level does your data protection officer report? i.e. CISO, CEO, etc.**

    The Data Protection Officer role falls within the remit of the Information Governance & Compliance Officer, who, in relation to all data protection matters, reports to the Senior Information Risk Owner (SIRO). The SIRO is a member of the Executive Leadership team. This is the highest level in the organisation – as specified by the legislation.