DORSET & WILTSHIRE FIRE AND RESCUE

Freedom of Information Request FOI 18 53

GDPR

Query and response:

1. Have you invested in technology specifically to comply with GDPR?

   No

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

   Our information security framework is based on ISO 27001.

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?

   We are in the process of doing this.

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?

   No, we use encryption for all our mobile devices.

6. As part of this audit, did you clarify if PII data is being stored on, and/or accessed by:

   a. Mobile devices **– No**
   b. Cloud services **– No**
   c. Third party contractors **– Yes**

7. Does the organisation employ controls that will prevent an unknown device accessing PII repositories?

   Yes

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.?

   Yes

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?

No

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

    Deputy Chief Fire Officer