ESSEX POLICE, FIRE AND CRIME COMMISSIONER FIRE & RESCUE AUTHORITY

Essex County Fire & Rescue Service

Meeting	**Performance & Resources Board**	**Agenda Item**	13
Meeting Date	30th October 2020	**Report Number**	
Report Author:	Assistant Director, Performance & Data Management		
Presented By	Deputy Chief Fire Officer (on behalf of Director of Corporate Services)		
Subject	**ECFRS Managing Data Breaches**		
Type of Report:	Information		

RECOMMENDATIONS

Members of the Performance & Resources Board are asked to note the arrangements that Essex County Fire and Rescue Service (ECFRS) has in place to manage data breaches and how this is reviewed and scrutinised through internal audit.

BACKGROUND

In April 2017, Information Governance Service (IGS) from Essex County Council (ECC) were commissioned to conduct an Information Governance Audit/Gap Analysis. This was to assist ECFRS with their preparation work to move towards GDPR compliance. The opinion issued through the audit at the time was, No Assurance. This led to the Information Governance Board led by the SIRO to establish an action plan that would enable the service to be compliant with GDPR and meet the Data Protection Act 2018 legislation.

It was quickly identified that ECFRS did not have a data breach handling process or record of data breaches and therefore one of the immediate actions contained with the plan was to address this and educate staff on the process and the importance of reporting breaches.

In August 2019 IGS returned to ECFRS to conduct a follow up Audit (Appendix 1) this audit report shows the previous RAG assessment for each area covered and the revised RAG for each area following the audit in 2019. The opinion issued in August 2019 was Adequate Assurance which demonstrates that considerable progress had been achieved.

Whilst the IGS audits have been used as a tool to identify progress required and measure the progress achieved, ECFRS has incorporated GDPR Compliance Audits into the annual audit plan. GDPR compliance is audited by RSM who do stipulate that they are not able to provide an opinion but will make recommendations for management action.

RSM have conducted two GDPR compliance audits at Essex Fire in May 2018 and April 2020. All RSM Audit reports are presented to the Audit Committee for scrutiny.
The data breach process has been audited as part of all RSM and IGS audits that have been conducted at ECFRS. Through the April 2020 RSM Audit the following management action in relation to data breaches was identified and agreed: -

Data Breaches - Management Action 12

Management will update the data breach guidance to include:

- The definition of what constitutes a data breach;
- The potential outcomes including:
  - Fines for reporting data breaches after longer than 72 hours; and
  - Fines by the ICO for data breaches up to 20 million euros or 4% of annual turnover.

Management will also conduct a data breach exercise (this could be combined with wider business continuity efforts) and utilise the results to further inform data breach guidance.

The training package for staff on Information Governance has been updated to include the guidance on what constitutes a data breach and details of fines that could be incurred.

The Service Leadership Team (SLT) have recently undertaken Information Governance training for leaders and a data breach exercise is being arranged to test this. This will be reviewed by RSM at the follow up audit.

Our reporting and handling of data breaches and information security incidents process, details how decisions are made by the DPO and SIRO on which breaches need to be reported to the ICO. It also details the process that will be followed, should a major data breach occur. The response to the data breach is co-ordinated through our current Critical Incident Team (CIT) structure. The handling of data breaches and information security incidents procedure has been defined within our data breach plan and identifies key stakeholders that would be contacted to action as part of CIT.

Data Breach Log

The Service holds a data breach log and for each data incident/breach the following information is recorded: -

Reference
Date of Data Breach
No. of people affected
Nature of Breach
Description of Breach
How you became aware of the breach
Description of data
Consequence of breach
All individuals informed?
Remedial Action
Other Regulators Informed?
Date ICO notified
Link to case folder.

BENEFITS AND RISK IMPLICATIONS

Under GDPR any organisation who fails to comply and/or suffer a data breach could face a fine. In the most serious cases, this fine could be up to 17 million euros, or 4% of annual turnover.

This upper limit far exceeds the current maximum fine of £500,000 allowed under the Data Protection Act.
When deciding whether to impose a fine following a data breach, the ICO will consider (amongst other things) the following:

- The severity and duration of the data breach

- Whether the breach was intentional or negligent
- If the organisation has had a previous data breach
- The type of personal data involved in the breach
- Whether the breach affects the rights and freedoms of the individuals affected

It should be noted that fines are extremely rare and the Information Commissioner's Office (ICO) advises that GDPR is less about fines and more about putting the privacy of the public first and advises that fines will always be a last resort.

There is of course the consideration of reputational damage and the impact of loss of confidence that poor data management and data handling can have if not complied with in line with Data Protection legislation.

FINANCIAL IMPLICATIONS

The financial implications are those highlighted above in relation to potential fines.

EQUALITY AND DIVERSITY IMPLICATIONS

There are no additional Equality and Diversity implications created by this report.

WORKFORCE ENGAGEMENT

There is a mandatory E-Learning module that all staff are required to undertake to ensure that all employees have an underlying knowledge of their responsibilities to ensure that they comply with Data Protection and GDPR legislation.

Spot checks are carried out by members of the Information Governance team to ensure that private and confidential information is stored securely and not open to general view.

LEGAL IMPLICATIONS

Non-compliance against the Data Protection Act 2018 and GDPR Legislation could result in legal action being taken against ECFRS.