Data Protection Compliance

The group discussed whether Element 9 (Data Protection) was still required as a distinct, separate Element or whether compliance with Data Protection legislation could be demonstrated throughout the other Elements of the RMP (especially Elements 5, 6 and 14). Compliance statements and evidence could be provided in these Elements to demonstrate the arrangements in place.

Also discussion around whether there was actually a need for the RMP to include Data Protection at all given that this was the responsibility of another regulator. If Data Protection is to continue to be part of an authority's RMP, what should the Keeper be asking for in terms of compliance statements and evidence? These should also tie in with what is required by the ICO so that what the Keeper requires doesn't contradict Data Protection legislation or leads to a different level of compliance. Discussions required with ICO.

RMP Elements – a lot of them are inter-related and it's important to try not to duplicate work to lessen the burden on authorities. A comprehensive Information Asset Register (IAR) was seen as a useful tool for internal business use and for aiding compliance and should be used to list categories of records containing personal information and could be used to identify the reasons for processing. The group discussed the possibility that a comprehensive IAR could be used to cover a number of elements (4, 5, 6, 7, 8 and 14).

The group felt that it was important that the Keeper defines what is required for authorities to comply with Element 9 and the types of evidence required. It was quite 'light' in terms of evidential requirements compared to other Elements. Registration with the ICO was now seen as more of a financial transaction than registering categories of personal information and reasons for processing-less weight as evidence for RMP.

It was asked whether Element 9 should be more robust in asking for compliance with other Elements (such as retention schedules and destruction).

PRSA Data Protection flipchart notes

Should Data Protection remain as a separate Element? On balance the group thought yes, but most Elements and their evidence overlap and it may be possible to show compliance through the other Elements.

Removal of Element 9 could be seen as 'swimming against the tide' of increased Data Protection visibility.

The Keeper should define what Element 9 covers and what evidence is required.

Agreed RMP = a record of GDPR accountability/compliance?

Information Asset Registers satisfies Element 4 (BCS) and records of processing.

Challenges for smaller organisations without a DPO.

Registration with ICO is now meaningless, authorities will need to submit different evidence

Authorities don't want to re-submit RMPs until the Model Plan review is completes.

ICO views on Data Protection requirements of RMP required.

The PRSA Assessment Team should experiment with drafting of new Model Plan – once detail required under other Elements becomes clearer, the need for Element 9 will be clearer.

Most authorities have several compliance regime requirements – want to avoid duplication of effort.

Element 9 = currently light touch and public facing-needs to be more robust?