Data Protection Board
Board Notes
16.6.2022

Attendees:

[redacted] Art 25

Absence:

[redacted]

Agenda points:

1. Privacy Compliance Report:
   - Update
   - Interpretation of Statistics
2. Third party suppliers - [redacted]
3. SAR cover notes.
4. JOIC registrations issues.
5. AOB.

Forum Notes:

Call recording:

- [redacted] informed the meeting that the call would not be recorded due to issues raised by JOIC in relation to lack of guidance on call recordings. Full meeting notes would be circulated instead.

Privacy Compliance Report:

- [redacted] gave thanks on the Privacy Compliance Report feedback for those that had done it.
- [redacted] noted that there had been some differences in interpreting the report statistics so ran through what was required for each of the categories on the report as follows (this table will be saved in the DP Board Teams Files):

Statistic	Interpretation	Record keeping obligation
- number of SAR's received that quarter	Total number of requests you have received in that month. Not just those that are still open.	DPU track those submitted through website but may not be aware of any submitted directly to DGO
- number of overdue SAR's responses	Response did not go back within 30 days or extension period if extended	DPU track those aware of and I am beginning to track but often not fully informed e.g. extensions

- number of complaints received from JOIC	Where a data subject has complained to JOIC directly and they have issued it as an investigation. Includes Conciliation/amicable resolution, enquiries, formal investigations and any complaints relating to breaches or alleging breaches.	Tracked by DPO if JOIC include me but don't always
- issues causing delays in responses	Free text. Anything want to highlight to ELT - e.g. Lack of resource, lack of efficient data gathering tools, complexity of requests.	DGO only
- number of DP breaches reported internally	Number reported either directly to DGO or in SIR/Datex. SIR will record all security incidents but we are only interested in those that are personal data breaches. No breaches of the DP law.	DGO only
- number of DP breaches reported to JOIC	Of those reported internally, how many were then notified to JOIC. Don't include any complaints to JOIC that data has been disclosed/breached - only those that we reported used SRDB	Tracked by DPO but only if DGO notifies me
- issues causing breaches	Free text. Both internal and JOIC. Anything want to highlight to ELT e.g. Staff turnover, lack of training, culture	DGO only
- number of new high risk data processing activities commenced	So anything where screener revealed need for full DPIA. Report it in month that reported to DPU so can track workload or DPU/DPO.	DPU track the screeners if submitted. Will be tracked on central system when up and running
- number of DPIAs completed and signed off.	Only DPIAs that have been signed off by DGO and DPU have logged as final. If with DPO for further review or comments have been made, it is not 'signed off'. Report in month that DPU confirmed final.	DPU track those aware of. Will be tracked on central system when up and running
- number of DPJL breaches (e.g. processing has commenced before DPIA complete, data sharing with no DSA or DPA in place)	Not DP breaches, breaches of legal requirement/policy. Doesn't have to be 100% accurate but should try to track where anything material has either been reported as part of complaint (and upheld) or you have noticed anything particularly concerning, should report these	DGO only
- number of DPIAs requiring consultation with JOIC	Only those that DPO advises require consultation. Report in month which final 'signed off' DPIA sent to JOIC, not month which they respond/project goes live.	DGO only

Third party suppliers:

Art 25 & 35

DPIAs

- [redacted] raised query re DPIA for systems used government wide and wished to receive clarity on who should be providing the review and drafting of these DPIAs. Does the review of the systems administered by M&D sit with each DGO or centrally with M&D. Do departments or M&D hold a list of 'corporate platforms' or list of what has gone through MERS / NFRs?
- [redacted] stated that they have regular meetings with their business enablement managers for their department in which they consider the systems in use and if they are acceptable from an information security and DP perspective, to ensure there is a review process in place and flag any risks.
- [redacted] confirmed that CLS are launching lots of online forms and she does a DPIA for each. All use Granicus, which is a corporate platform. Have agreed with DPU that, instead of drafting a DPIA for Granicus, the risks of using the platform are considered within the survey DPIAs and standard wording is included to cover the known risks. Also working on creating standard wording to cover risks identified with access permissions due to active directory not being up to date to ensure this point is covered within each DPIA.

Art 25

- [redacted] asked [redacted] the question if she would be happy that a list of corporate platforms be created. [redacted] stated that she would like this to be put in place in the future. [redacted] pointed out that latest version of the DPIA template includes additional wording on TOMs and working with [redacted] to iron out when can include standard wording for a 'corporate' system rather than having to re-assess them each time [redacted] also stated that even though there may be an 'approved' list, it should not be relied upon as a blanket approval for all uses. The activity the system is being used for in each instance should be assessed. The system risks should be highlighted in the DPIA and consider the implications for the activity the system is being used for. Art 25
- **[redacted] to feedback re work with [redacted] on the due diligence for corporate systems**

SAR cover notes:

- [redacted] mentioned that the SAR cover note is now live to be used and advised promoted its use going forward.
- [redacted] reminded meeting that the cover note template is in the DP Board Files under 'templates'. **DGO's to contact [redacted] if not aware of the cover note.**

JOIC registrations issues:

- [redacted] raised ongoing issue with the JOIC registration process. Amendments and deletions are not being processed unless save changes after each and every change. Can't do bulk changes. This has affected the accuracy of the registrations being entered by [redacted]/DPU. [redacted] working with JOIC to rectify. [redacted] **asked DGOs to check their registrations and report back to [redacted] if they are not correct.** Art 25
- [redacted] informed DGOs that JOIC are still interpreting registered business names as the data controllers. [redacted] advised that the department is the registered controller and this has not changed. Conversations on this understanding is still ongoing with JOIC to ensure that there is clarity on naming conventions. In the meantime, [redacted] advised that if JOIC approach a department regarding this, the DGO should reiterated that the Department is the controller, not the registered business name.

AOB:

Crisis event

- [redacted] Art 42(a)
- [redacted]

Amicable Resolution

- [redacted] is still chasing the slides on the amicable resolutions from JOIC. These will be circulated once they are provided. Art 25

Call Recording Guidelines

- [redacted] queried Teams meeting recordings and the issues re its use
- [redacted] stated that guidance was being drafted by [redacted] and will be reviewed by [redacted] once drafted.
- [redacted] queried whether should stop recording calls. Confirmed JHA record all SLT meetings. [redacted] stated no change to business practices yet – need to consider its use in depth rather than provided a rushed outcome. Better to have guidance and policy than blanket rules. Also need to consider the scope of any policy put together.
- [redacted] asked [redacted] why they choose to regularly record meetings. [redacted] stated as this was used to replace minutes so only actions need to be taken and that its helpful if you cannot attend and wish to view the meeting at a later point. [redacted] agreed that should be used in place of verbatim minutes but not so can draft minutes from recordings. Art 25
- [redacted] raised concerns that SPPP has capability issues at the moment with meeting minutes so needs to record calls. [redacted] confirmed that nothing should change yet but guidance does need to be put in place for consistency. [redacted] **will circulate guidance once drafted.**

Point raised in chat after the meeting

- [redacted] - "I am aware that the DPIA template being used by the CPMO is not the corporate one. It's very similar but not the same. Is this intentional?"
- Ans: [redacted] responds – "No it's not intentional. We had asked them to switch to using the link to the DPIA so they would have the latest version and we didn't have to update them every time we made a small change, but I guess they have.t done that yet. **I'll pick it up with them**".

Actions and decisions:

DGO's:

- Provide list of approved third parties to DPO if this exists for the creation of a central list which can then be reviewed.
- Check JOIC registrations and report back to [redacted] if they are incorrect.
- Brief DG's on when should involved DGO in 'global' incident
- Consider documents needed in event of incident that takes out emails/systems

[redacted]

- Compile list of corporate platforms when received from DGOs.
- Provide feedback and a playbook in the event of a corporate crisis such as a global data breach.
- Feedback response from Stuart re due diligence on 'corporate' systems.
- Circulate Amicable Resolution slides once they are provided.
- Circulate Call recordings guidance once drafted
- Request CPMO update DPIA template.

[redacted]

- Feedback to Commercial concerns raised re due diligence from DP perspective and continue to work with them on due diligence questionnaire.

[redacted]

- Send [redacted] list of 'pre-approved' suppliers