Questions from 5/22/24 GDPA Workshop

Q1. When is the ombudsperson expected to be hired/appointed?
The expectation is in the new couple of months. (June/July)

Q2. How can we hope to get larger agencies who only accept adhesion contracts (only their terms) to include the required language?
Our recommended language mirrors standard and fair requirements that are typical to see in other states as well as regions that the bigger agencies or companies are typically also operating at, so they are likely to be compliant already (for example with the requirement not to use the data for any other purpose than providing services under contract, timely breach notification, or destruction/return of the data). But if entities refuse to adopt our clauses and don't have corresponding ones in their contracts/T&C's I'd consider that a significant redflag and consult with your legal counsel to see if further negotiation is possible and if not then with your leadership to see if an alternative to the entity is available. Especially if they don't have a limitation on use of data and adequate breach notification.

Q3. The GDPA defines data selling as follows: 18(a) "Sell" means an exchange of personal data for monetary consideration by a governmental entity to a third party." You mentioned there is an additional component: "when the governmental entity uses that monetary consideration to finance their activities." Should we interpret this section of the GDPA to mean that selling data includes both the exchange for monetary consideration and the use of that money to fund governmental activities? No, this is not an additional component, it was a real life example we have seen in practice and that is not allowed going forward. Entities are not allowed to fund their operation by sale of personal data.

Q4. Number 4 states that entities cannot share "personal data" unless permitted by law. For many of us, a lot of our documents are considered "public" under GRAMA. So does GDPA prohibit governmental entities from sharing public records in light of the GDPA being more restrictive? No, it does not outright prohibit it. As long as there is a legitimate reason to share it and it is done in a way law permits, (example: under a contract, with appropriate notice) the data can be shared. Also GRAMA is specifically named as the more restrictive/specific law in the GDPA so it would prevail in those more restrictive cases.

Q5. Does the GDPA apply to aggregated, de-identified, or anonymized data processing?

No, BUT, the aggregation, de-identification and/or anonymization must be done at a standard that does not allow reverse engineering / distinguishing one individual from another. Basically as long as it cannot be linked to an identifiable individual, it would not be personal data.

Q6. What does "Data Sharing" encompass under the GDPA?
Provision of access to another party/person/entity.

Q7: Question about 2025 First Annual Privacy Report: What information do we need to report to the Privacy Officer, and is there any template available so we can start capturing the information on May 1, 2024? Do we need to include personal data we share with third-party vendors?
Template is available (see the toolkit) and yes you need to share the type of personal information and types/classes of persons/entities you share it with and why, including vendors.

Q8: Normally it is any UNINTENTIONAL disclosure that is a breach.
Or "unauthorized"
Unauthorized yes, but both unintentional or intentional IMPROPER disclosures would be a breach.

Q9: Would buying a Data Protection Software and turning it on "count" as a Program ?
I would have to see which one you have in mind, but it would most likely not be a holistic program. Program has to include individual components such as training, monitoring, measuring, and driving compliance. Simply having a software in place may not be enough, while it can be a very helpful tool to support all these individual components. Examples: OneTRust is an effective software that helps manage privacy risk but wouldn't replace a privacy program. Big ID is an effective tool for data management and classification, Colibra for overall Data Governance, but I cannot recall a software that would outright replace a privacy program.

Q10: What is included in "personal data". Is this employee information as well? Such as new hire information?
Yes, personal data may include data of your clients (the population you serve), employers, volunteers, and/or vendors. In short: any data that can identify a living individual regardless of who the individual is would be personal data.

Q11: How about we just don't sell it at all we are government entities
Agreed, that's what the law aims at, no selling of personal data at all.

Q12: Can you use the same notice for multiple applications/licenses or do you need separate notices for each separate purpose?

Yes, as long as the notice is still easy to understand/find/read and the individual purposes are clear. Recommended length is between 1-2 pages/ 1-2 scrolls on a mobile device. Tiered approach can also be used, where the most important one or two sentences “We only use your data to provide services you requested on this form and the law permits us to and we don't monetize or otherwise improperly share your data. If you don’t provide the data we may not be able to furnish you with the services you request” with a link to the full notice. Feel free to send us your notice for a review.

Q13: Isn't a breach defined as more than 500 so the entire question is flawed
500 impacted people makes it a “reportable” breach, breach itself does not have a limitation based on how many people it impacted, but rather how likely it is a compromise of their data happened.
;
Q14: As of when is having to provide breach notification applicable?
May 1st 2024.