GDPR Data Protection Framework

Table of Contents

Annexes

Introduction

As an advertising exchange platform providing services and collecting personal data in Europe, district m has brought its personal data management practices in compliance with the General Data Protection Regulation (GDPR). This document describes district m's personal data management under GDPR.

The GDPR will come into effect on 25 May 2018. There is no grace period and organisations will need to comply with the new rules from this date. district m is in compliance with its provisions.

The GDPR is a major overhaul of current law. One of the key changes is that Supervisory Authorities (the regulators responsible for enforcing GDPR) can impose fines of up to 4 per cent of global turnover or €20,000,000, whichever is higher, for breaches of the GDPR. Specifically, the GDPR focuses on organisations having appropriate data protection governance in place with a real emphasis on accountability.

Purpose of this Document

The purpose of this Document is to highlight the main principles and changes under the GDPR implemented by district m through policies and processes in compliance with the GDPR. Each section describes a different principle and/or rule under the GDPR. The "Actions" sections throughout the document identify measures taken by district m to ensure compliance with the GDPR.

Annexes contain the following policies and mechanisms under GDPR:

- Annex A: Personal Data Protection Policy
- Annex B: Personal Data Retention Schedule
- Annex C: Incident and Breach Response Process
- Annex D: Data Protection for Contractual Agreements
- Annex E: Data Protection Governance Framework

Territorial Scope

The GDPR will apply to any organisation processing personal data from individuals in Europe. district m has clients and users in Europe.

Actions:

- district m has adopted the necessary policies, processes, practices and contractual clauses to comply with the GDPR.
- Content of district m's databases storing personal data has been reviewed to ensure compliance with the GDPR. Specifically, making information about personal data protection and management at district m concise, transparent, easily accessible and clear.
- district m will monitor compliance with the GDPR obligations as set out in its policies and processes described in the Annexes to this document.

Definitions

Summarised key definitions from the GDPR:

Key definition	Meaning
Personal Data	Any information relating to an identified or identifiable natural person.
Controller/Data Controller	The organization which determines the processes and means of the processing of personal data.
Processor/ Data Processor	The organization which processes personal data on behalf of the controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processing	Any operation or set of operations which is performed on personal data.
Profiling	Any form of automated processing of personal data to evaluate certain personal aspects of an individual; in particular to analyse or predict aspects concerning personal preferences, interests, reliability, behaviour, location or movements.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately. This means a process of de-identifying data, hashing or applying dummy IDs to minimise it and remove identifiers.
Special categories of personal/sensitive data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Actions:

- district m is a data controller with respect to its websites and applications where individuals directly provide Personal Data to district m when signing up to utilize the application received from our clients as part of the services we provide.
- district m is a data processor with respect to Personal Data it processes for publishers and advertisers.
- district m performs profiling and other forms of automated decision-making on the personal data it holds. This is high level profiling and it does not involve sensitive personal data of individuals.
- district m anonymizes information for reporting purposes.

Principles

Data Protection Principles under GDPR set out the main responsibilities as follows:

1. Lawful, fair and transparent process;
2. Specific and legitimate purposes for collection and process;
3. Limitation to data necessary to fulfill the purposes;
4. Accuracy of data;
5. Retention only as long as necessary;
6. Security of data;
7. Accountability of data holder.

Personal data should be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

Actions:

- district m collects and processes personal data of individuals, such as IP address or cookies, strictly as necessary to provide its services.
- Personal data is collected by district m, processed and aggregated in anonymized form for statistical and machine learning for optimizing purposes.
- district m provides clear information in its Privacy Policy, which is accessible through its website and attached at Annex A.

b) personal data must be collected and processed exclusively for the purposes as stated upon collection;

Action:

- Where district m directly collects personal data, it uses a form where individuals proactively provide their data.

c) data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

Action:

- In collecting Personal Data, district m ensures it only collects the minimum data required. This includes billing and mailing address and account information as provided by the user. With respect to credit card information, it is tokenized and only the token and the four last digits of the credit card are stored.

d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

Action:

- district m ensures that all data it collects is accurate, in particular through syncing account information with Microsoft CRM via Microsoft Queue System.

e) GDPR requires personal data be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed;

Action:

- district m retains personal data transferred by customers for 60 days or not at all. Data is destroyed after this period.
- Credit card information is immediately tokenized.
- Data Retention Schedule is at Annex B.

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

Action:

- district m protects Personal Data in accordance with the Security Plan.

g) The controller shall be responsible for, and be able to demonstrate, compliance with the principles;

Action:

- Accountability is ensured at district m with an independent data protection law advisor to ensure and demonstrate compliance with GDPR, including through policies, procedures, training and awareness.

- district m has adopted incident and breach report forms to document all incidents for rectification or audits, attached at **Annex C**.

Data Governance

Data Protection Officer

The GDPR introduces a requirement for some organisations to appoint a Data Protection Officer (DPO) to oversee their organisation's data protection activities and compliance with the GDPR.

Because designating a DPO is a good practice in data protection, district m has appointed Chantal Bernier, National Leader, Privacy and Cybersecurity, Dentons Canada LLP.

The DPO functions include:

- reporting on compliance with data protection law to senior management;
- informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, training staff and conducting internal audits as necessary;
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees and customers);
- advising the organization in case of a breach.

district m's Obligations

Consent

GDPR describes "consent" as the freely-given, specific, informed and unambiguous indication of the individual's wishes. In certain cases, explicit consent is required which means consent that is very specific as to data collected, purposes and disclosures.

Action:

- district m obtains express consent when collecting cookie or device data from customers visiting its websites. A website Privacy statement is prominent on district m's websites. It contains a link to district m's Privacy Policy. Both are attached at **Annex A**.

- district m Data Flow explains the process by which district m collects personal data from users and clients.

Records of processing

Because district m's processing of personal data in the EU is not occasional, district m maintains records of its processing activities in compliance with GDPR.

Actions:
- district m will provide records for processing upon request.

Rights of Individuals

General

Individuals' existing rights are substantially strengthened under the GDPR. Of relevance to District m are the right to individual access and the right to rectification.

Individual access and rectification rights

- Individuals have the right to obtain access regarding the personal data held on them as well as information regarding storage abroad; they also have the right to complain to a supervisory authority.
- Controllers must respond to access requests without undue delay and within one month at the latest. This must be done free of charge to the data subject.
- If the request is made electronically, the personal data must be provided in a commonly used electronic format.
- Data controllers must also rectify inaccurate data and provide a supplementary statement if data is incomplete.
- Data controllers must give reasons if they refuse the request.

Action:
- district m has the technological means to extract personal data to respond to an individual request for access to that data where it is explicitly provided and that the user demonstrates rightful ownership. Should district m not be in a position to provide access, district m will provide reasons.

Challenging compliance

- Individuals have the right to challenge compliance with data protection principles and data controllers and processors have the duty to cooperate with supervisory authorities in investigations in this regard.

Action:

- district m has adopted mechanisms to address access, rectification and challenging compliance as described in its privacy policy at Annex A.

Privacy by design/default

The GDPR expressly legislates for what has been considered best practice in data governance. Among the new data governance obligations are the obligations of:

- *Privacy by design*: to take appropriate measures to integrate the GDPRs data protection principles into data processing operations – taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the severity and likelihood of the risks posed to privacy. This includes, for example, pseudonymisation. This obligation applies to existing and new processing systems.

- *Privacy by default*: to take appropriate technical and organisational measures to minimise the use of data, with regard to each specific purpose of processing, as the default position. Minimisation applies to the amount of data collected, extent of processing, storage period, and accessibility. In particular, personal data should not be made accessible, without the individual's intervention, to an indefinite number of other individuals. This also applies to existing and new processing.

Action:

- district m has reviewed its processing operations and data flows and further reduced the personal data it stores to the strict minimum to perform its service.

- district m Data Retention Schedule, attached at Annex C, builds in privacy by default through minimal retention periods.

- district m will impose on suppliers, through contractual means, an obligation to take the above measures where appropriate.

- district m will require external counsel to monitor and report on EU regulations guidance on GDPR for ongoing compliance.

Security

The GDPR requires controllers and processors to adopt certain security measures to prevent against, and mitigate the consequences of, data breaches.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The GDPR introduces the following data security requirements:

- All data controllers, as district m is for its users, and processors, as district m is for its clients, must implement, according to the level of risk associated with their processing activities, all appropriate technical and organisational measures to ensure data is protected. These measures can include

pseudonymisation, encryption, back-up data sets, etc. The GDPR requires controllers/processors to regularly test and assess the efficacy of these measures.

- All controllers must maintain a register of all data breaches, comprising the details of the breach, its effects, and any actions taken, in order to demonstrate compliance in the event of an audit.

- In addition, controllers must maintain a record of data breaches to be accessed by the Supervisory Authority upon request.

Action:
In case of a data breach:

- Data processors must notify the data controller, in this case, district m's client, without undue delay in the event of any data breach, as soon as it becomes aware of it.

- district m will require that its processors comply with this obligation.

Data controllers must notify:

- The relevant supervisory authority without undue delay (and no later than 72 hours) after becoming aware of a data breach that could result in a risk to the rights and freedoms of individuals. Most data breaches will need to be notified.

Action:
- district m will notify users, without undue delay after becoming aware of the breach, except where:
    - the data is unintelligible to anyone not authorised to access it (e.g. the data is encrypted);
    - measures ensure the high risk to individuals is no longer likely to materialise;
    - notifying the individuals concerned would involve disproportionate effort. In this instance a public communication would suffice, provided the individuals concerned are informed in an equally effective manner.
- When reporting a data breach, the organisation must outline:
    - the nature of the breach, including (where possible) the categories and number of individuals affected, as well as the categories and number of personal data records concerned;
    - the name and contact details of the organisation's DPO (or other contact) where more information may be obtained;
    - the likely consequences of the breach;
    - the measures taken (or proposed to be taken) to address the issue, and any measures taken to mitigate adverse effects.

Actions:

- district m has a comprehensive Security Plan.
- district m has adopted the Breach Response Plan attached at Annex C.
- district m enters into contractual agreements with its business partners. These contracts contain clauses with respect to the protection of personal data.
- Prior to entering into a contract agreement, district m makes inquiries into its suppliers' practices with respect to personal data protections and compliance with the GDPR, to ensure that personal data flowed to that supplier is protected in accordance with the provisions of the GDPR.

Contractual obligations

Requirements prior to engaging processors

GDPR requires that in engaging processors or sub-processors, an organization will only select processors which:

- provide sufficient guarantees for implementing technical and organisational measures to ensure processing meets the requirements of GDPR and protects individual rights;
- only engage sub-processors pre-approved by the controller; and
- enter into a contract with the controller which satisfies the requirements of GDPR and which sets out:
    - the subject matter and duration of the processing;
    - the nature and purpose of the processing;
    - the types of personal data and categories of data subjects; and
    - the obligations and rights of the controller.

Processor contracts

GDPR contains prescriptive requirements regarding the detail of what must be covered in a contract with a processor, as follows:

- The processor only processes data on documented instructions from its customers;
- Employees authorised to process the personal data are subject to obligations of confidentiality;
- Measures ensure a level of security appropriate to the risk (e.g. including encryption and pseudonymisation of data) and assists customers in meeting security obligations;
- The processor provides information and contributes to audits to demonstrate compliance;
- The processor will assist its customer, should the customer require approval from a regulator regarding its processing activities; and

- The processor implements measures to assist its customers in complying with the rights of individuals.

Action:
- district m has reviewed its contractual clauses for compliance with personal data transfers in GDPR. They are found at **Annex D**.

Processor obligations

The key obligations of processors under GDPR applicable to district m include:

- record details of databases and of any international transfers of personal data, including details of the relevant safeguards in place;
- provide a general description of the security measures in place to protect personal data;
- cooperate with requests from regulators when needed;
- notify controllers of data breaches without delay; and
- appoint a DPO if the processor meets the relevant criteria.

Action:

- this document and its annexes provide details of district m security measures, contractual clauses for the transfer of Personal Data and breach response plan.
- district m has identified a data protection law advisor to ensure implementation of GDPR.

Processor liability

Under GDPR, processors will have direct liability to individuals affected by a breach.

If a processor's processing activities have caused harm to an individual and it can be shown that the processor has: (i) not complied with its processor obligations under GDPR or (ii) acted outside the instructions of the controller, the processor will be liable to that individual for the damage caused.

It should be noted that controllers and processors may also be held jointly and severally liable to individuals for the entire damage where they are involved in the same processing causing harm. Harm includes non-pecuniary loss, such as distress. Controllers or processors (as relevant) can claim back the amount paid to individuals which corresponds to the harm caused by the other party.

Action:
As described at **Annex D** in district m's Data Protection Contractual Agreements, district m:

- conducts data protection due diligence on sub-contractors prior to engagements, attached at **Annex D**.
- has prepared template GDPR-compliant clauses to insert within agreements with sub-contractors, found at **Annex D**.

- monitors security measures of sub-contractors to assess for continued compliance with GDPR requirements as stated in its contractual clauses found at **Annex D**.

- has appointed Chantal Bernier, National Leader, Privacy and Cybersecurity, Dentons Canada LLP to monitor contractual compliance as described in the Data Protection Framework at **Annex E**.

- addresses cooperation on breach response policy and procedures as described in the Incident and Breach Response Process at **Annex C**.

Data Transfers

Transfer restrictions

There is a general restriction on transferring personal data outside the European Economic Area (EEA). The GDPR confirms this rule but removes certain administrative requirements.

Action:

- district m contractual agreement clauses at Annex D ensure that processes are set up so that new data flows from its EU customers are compliant and assessed on an ongoing basis.

- district m transfers data to the US through Microsoft, Amazon and Google under the EU-US Privacy Shield.

Personal Data Protection Policy

This Policy provides information regarding:

- district m's management and protection of personal data,
    1. Collected from its **employees** for workforce management purposes,
    2. Collected from **website visits** for the purposes of operating and improving the websites,
    3. Processed for district m **clients** under Service Agreements (SA)
    - o In relation to,
        - Collection
        - Disclosure
        - Transfer
        - Security
- the process to obtain individual access, rectification, as appropriate, of one's personal data held by district m

1. MANAGEMENT AND PROTECTION OF PERSONAL DATA

1.1 Collection

There are three ways in which personal data, meaning information about an identified or identifiable individual, is collected or processed by district m:

4. district m collects and processes personal data obtained directly from its **employees** for the purposes of human resource management including hiring, deployment, compensation, benefits, leave management, performance management, discipline and termination, as well as emergency contact. district m has no employees in Europe.

5. district m processes personal data **on behalf of its clients** according to what clients transfer to its platform.

6. district m collects personal data through visits to its **websites.**

With respect to its employees, district m collects personal data as required by taxation law and as necessary to manage the workforce and contact the employee, including:

- Employee's full name and social insurance/security number
- Personal address
- Birth date
- Gender
- Position
- Work schedule
- Hours worked

- Wages, including basic, overtime and incentive pay
- Total earnings
- Legally applicable deductions
- Date of payment and the pay period covered by the payment
- Performance assessment
- Date of end of employment
- Disciplinary measures and termination as the case may be.

Should Diversity and Equality programs bring district m to collect special categories of data, such as ethnicity or race to ensure fair representation in its workforce, such information would be given voluntarily and with express consent of the employee.

With respect to its clients, district m processes the personal data transferred by the client in the context of the SA and strictly under instructions of the client.

With respect to websites, district m enables third parties such as Google, Facebook and Appnexus to collect device and session info of users visiting its websites. The personal data is used to obtain information regarding Web site usage to tailor it to user needs.

In order to obtain access to portions of the Web site, district m may ask the user to complete a registration form that identifies personal data or solicits comments. Upon registration, e-mail and other personal data are collected to allow the interface with the user. This is done with express consent of the user, prompted by a request to agree.

Information about the Privacy Policy is featured prominently and easily accessed from the websites.

1.2 Disclosure

With respect to all three types of personal data, district m does not sell or otherwise disclose the data it holds to third parties save in the following exceptional cases:

- Should district m receive a request from law enforcement authorities to provide personal data in its custody, it would only do so upon demonstration of lawful authority. If the data requested is held on behalf of a client, district m will consult the client unless it is prohibited to do so by law.

- Strictly as allowed by law, district m may disclose personal data to another organization where it is:
    - reasonable for the purposes of investigating a breach of an agreement or a contravention of the law that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;
    - reasonable for the purposes of preventing, detecting or suppressing fraud and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud;
    - necessary to identify an individual who is injured, ill or deceased, to a government institution or the individual's next of kin or authorized representative and, if the individual is alive, with notification to the individual.

- With respect to employee data, district m may disclose personal data if it is necessary:
    - to establish, manage or terminate an employment relationship, as allowed by law.

- in a prospective business transaction where district m has entered into an agreement that:
  - restricts the use and disclosure of that data solely for purposes related to the transaction;
  - protects the data by security safeguards appropriate to the sensitivity of the information; and
  - if the transaction does not proceed, the data is returned to district m or destroyed within a reasonable time.

1.3 Transfer

district m may transfer personal data to third parties it employs to deliver its services.

The transfer is solely for the purpose of assisting district m in its service delivery and under its instructions. The transfer is protected through contractual clauses that ensure compliance with data protection legislation at a compatible level of protection.

In relation to data held on behalf of its **clients**, district m will transfer personal data to a third party it employs only with approval of the client and in accordance with the SA.

district m stores data in the U.S. under the EU-U.S. Privacy Shield.

1.4 Security

district m stores data using advanced technology for internet security available today. In particular,

- **All data** is protected at the appropriate level for the varying levels of risks specifically through physical measures, such a secure areas, technical measures, such as encryption, and organisational measures such as access controls and due diligence in transferring personal data to processors.
- **All data** is retained only for as long as it is necessary for the purposes for which it was collected or transferred, in accordance with the Retention Schedule.
- **Data held on behalf of district m clients**, is secure and available only to registered users in the client's organization as follows:
  - User authorization is enabled through Company ID, User ID and password.
  - All access is password protected and using a secure connection.
  - All data is transmitted using a secure (encrypted) FTP protocol.
  - Data about district m employees or data from websites is kept secure and available only to authorized staff on a need-to-know basis.
- **On its websites,** district m uses cookies and its websites privacy policy describes the use, nature and extent of personal data they collect, as well as the purpose and the options to disable cookies with the consequences of doing so as follows:
  - "district m sets cookies (district m user identifier) on your computer to associate with equivalent identifiers from partner platforms as the only element representing a user across the platform, in order to enable district m to transact with 3rd party buyers and sellers of media inventory without having to communicate PII data.."

2. PROCESS TO OBTAIN INDIVIDUAL ACCESS AND RECTIFICATION TO PERSONAL DATA

In relation to employee data, district m responds to individual requests for access to one`s personal data, and for rectification as necessary, through the Data Protection Officer (DPO): Chantal Bernier, National Leader, Privacy and Cybersecurity, Dentons Canada LLP at Chantal.Bernier@Dentons.com. In relation to website data, district m responds to these requests through the DPO: Chantal Bernier, National Leader, Privacy and Cybersecurity, Dentons Canada LLP at Chantal.Bernier@Dentons.com.

- Within one month, free of charge, unless
  - the volume or the complexity of the request require a longer process, where district m will inform the requester, within one month, of the reasons for an extension and may charge a reasonable fee to cover administrative costs; or
  - the request is unfounded or excessive and district m may refuse the request with justification.
- If district m processes personal data about the requester, it provides access to the data and the following information:
  - the purposes of the processing;
  - the categories of personal data processed:
  - the third parties to whom the personal data have been or will be transferred under the employment of district m and their location;
  - the criteria to determine the period for which the personal data will be stored,
  - the existence of the right to request rectification or erasure of personal data and the process for it;
  - the right to object to processing, as applicable;
  - the right to lodge a complaint with a supervisory authority.

district m provides rectification as soon as possible within one month. Should district m refuse the request, it will provide justification.

3. PROCESS TO CHALLENGE COMPLIANCE

An individual about whom district m processes data may challenge compliance with data protection rights by filing a complaint with district m's DPO: Chantal Bernier, National Leader, Privacy and Cybersecurity, Dentons Canada LLP at Chantal.Bernier@Dentons.com.

CONTACT

For more information, contact district m's DPO: Chantal Bernier, National Leader, Privacy and Cybersecurity, Dentons Canada LLP at Chantal.Bernier@Dentons.com.

Personal Data Retention Schedule

DISTRICT M'S STORAGE OF PERSONAL DATA IS LIMITED TO THE STRICT MINIMUM NECESSARY FOR THE PURPOSE FOR WHICH THE DATA HAS BEEN COLLECTED.

district m has established the following schedule and procedures in order to retain personal data to minimal periods.

- Personal data transferred by clients is destroyed before 60 days.
- Personal data from website visits is anonymized before 60 days.
- Employee data is retained for the duration of employment, plus one year, to provide individual access if requested.
- Job applicants' data is destroyed upon completion of the recruitment exercise, except with express consent, for further consideration, where the duration of the retention period will be determined in seeking consent.

Incident & Breach Response Process

Definitions

Breach and incident:

- **Data Breach =** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, of personal data transmitted, stored or otherwise processed.
- **Data Incident =** a breach of security constituting a failure to follow data security policies or procedures *without resulting* in a breach of data.

Personal data means any information relating to an identified or identifiable individual.

Breach Response Core Team: frontline team to investigate, remediate, report and advise on a breach.

Chief Information Officer (CIO): responsible for:

- investigation, documentation and remediation;
- coordination of identification;
- documentation and remediation; and
- reporting to CEO on technological assessment of gravity of the incident or breach and remediation, as well as on possible individual harm;

External Privacy Counsel as DPO: responsible for:

- engaging core team;
- ensuring compliance with breach response obligations;
- advising CEO on legal implications, including advice on notification based on assessment of individual harm;
- liaison with client in case of breach of client data; and
- engaging full team as appropriate.

Breach response Full team:

Core team and,

Chief Executive Officer (CEO): responsible for critical decisions, such as,

- Breach notification upon recommendation of the external privacy counsel as DPO;
- Resource dedication to address breach; and
- Review of public communications material as the case may be.

Chief Financial Officer responsible for

- business continuity as needed; and
- management of breach expenditures as needed.

In addition,

In case of breaches of employee data,

Vice-President Human Resources: responsible for:

- assisting CIO in assessment;
- leading HR through assessment and remediation;
- assisting in notification as necessary.

In case of breach of client data,

Chief Information Officer: responsible for assisting External Privacy Counsel as DPO in communicating with client;

Vice-President, Marketing: responsible for brand management through the breach response.

External privacy breach counsel/DPO contact:

Chantal Bernier
D +1 613 783 9684
M +1 613 716 1976
chantal.bernier@dentons.com

district m's legal obligations in case of breach or incident regarding personal data

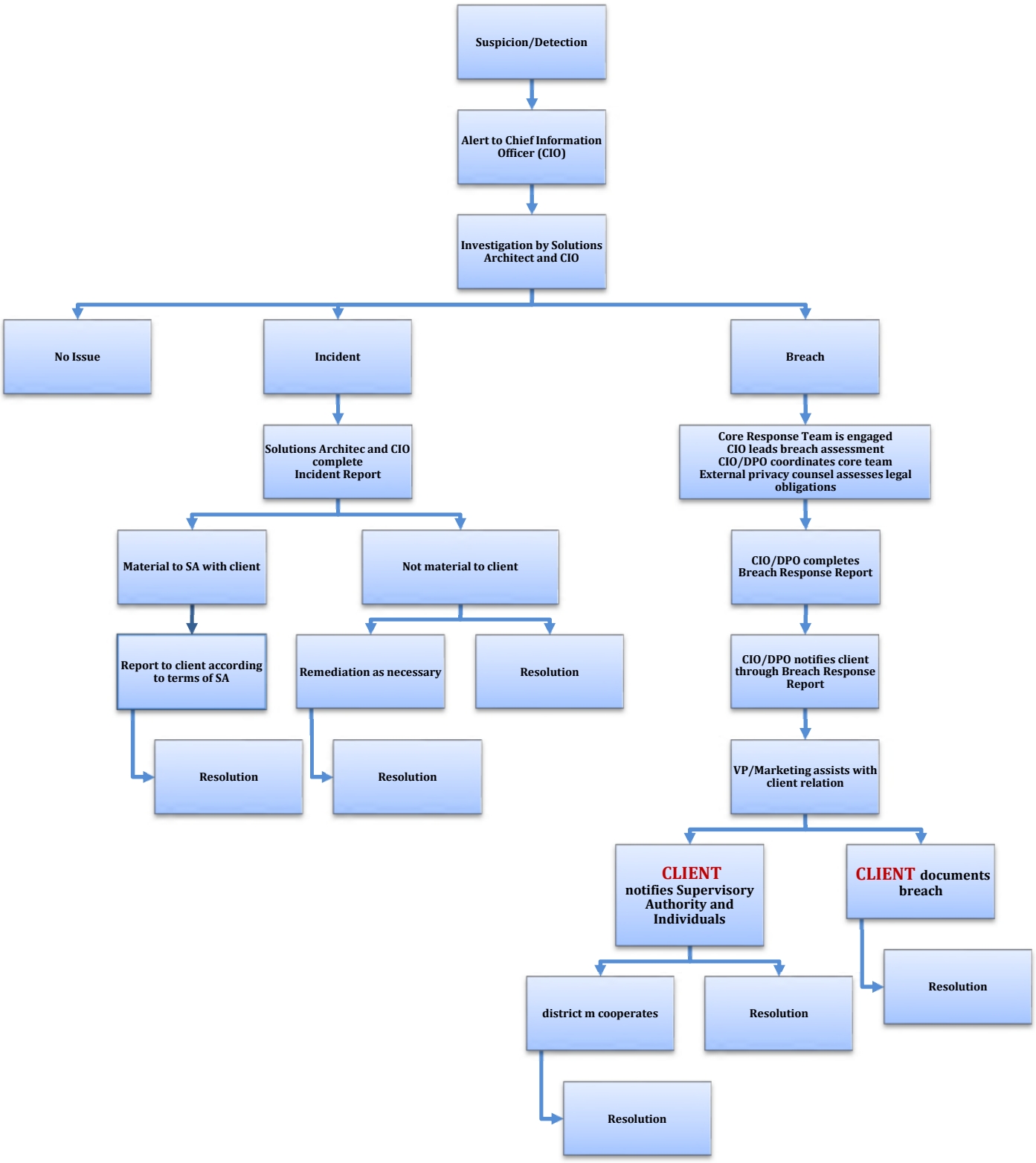
In Canada:

- Under amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) expected to come into force in 2018, district m has the obligation to, *as soon as feasible if it creates a real risk of significant harm to an individual*:
    - Report to the Office of the Privacy Commissioner of Canada (OPC);
    - Notify the individual - unless prohibited by law, for example if the data breached is covered by national security protection;
    - Notify any other organization if district m believes that organization may be able to reduce the risk of harm;
    - Maintain a record of every breach of security safeguards;
    - Provide the OPC access to those records upon request;
    - Notification to the OPC under the *Personal Information Protection and Electronic Documents Act.*
- Notification to individuals should
    - Contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps to reduce the risk of harm;
    - Be conspicuous and given directly as prescribed by regulation.
- "Significant harm" is defined as including *bodily harm, humiliation, damage to reputation or relationships, loss of employment, business of professional opportunities, financial loss, identity theft, negative effects to the credit record and damage to or loss of property*.

In Europe:

- the GDPR establishes a process where district m is considered a data processor – i.e. in relation to the personal data it holds on behalf of its clients.
    - In relation to a breach of personal data received from a **client,** district m will:
        1. Immediately investigate the breach.
        2. Notify the client without undue delay.
        3. Communicate and cooperate with the client as illustrated in Chart 1.

Chart 1 **RESPONSE PROCESS FOR SUSPICION/DETECTION OF INCIDENT OR BREACH OF district m AS PROCESSOR (CLIENT PERSONAL DATA)**



3.3 Steps

district m addresses data incidents and breaches as a priority.

Step 1. As soon as a data security event is suspected, whether a breach or an incident, the district m employee or contractor who suspects or detects it alerts the Chief Information Officer (CIO) to investigate in collaboration with the Solutions Architect.

Step 2.

- Should the CIO conclude that no incident or breach exists, the matter is resolved without further action.
- Should the CIO conclude that an incident occurred, it completes an Incident Report at Tab A, including recommendations for remediation as necessary.
- Should the CIO conclude that a breach occurred, the Response Core Team is engaged with the following composition and responsibilities:

Chart 3: FULL BREACH RESPONSE TEAM RESPONSIBILITIES

Officer	Responsibilities

Chief Information Officer (CIO)	• Acts as DPO
	• Initiates the Breach Response Process
	• Leads the team in
	  o breach assessment
	  o operations support
	  o completing breach report
	  o containment and remediation
	• Reports and advises on gravity of the breach as high, medium or low in accordance with Chart 4
	• Assigns or requests resources as necessary
	• Coordinates the Breach Response Team by calling regular reporting meetings
	• Reports the breach and remediation plan to the CEO
	• Advises the CEO on next steps
	• Drafts notification communications including notification as necessary
	• Provides advice for involving law enforcement agencies as necessary

Vice-President Finance & Administration	• Provides support for employee data breaches
CEO	• Decides on notification
Vice-President Finance & Administration	• Leads business continuity • Manages expenditure

VP Marketing	• If necessary, manages brand protection • Interfaces with the Media and Public as necessary. • Coordinates internal communications
Client Officer	• Assists CIO/DPO on client data breaches.

Chart 4: LEGAL RISK ASSESSMENT

Risk Level	Criteria
High	• High risk of significant harm such as o Bodily harm o Humiliation o Damage to reputation or relationships o Loss of employment business or professional opportunities, o Financial loss o Identity theft o Negative effects on credit o Damage to or loss of property • Number of affected individuals • Sensitivity of data affected (SIN, date of birth, medical leave data, performance assessments) • Requires notification of individuals and regulator, and documentation
Medium	• Breach of personal information where o Appropriate technical and organizational protection measures were implemented that rendered the personal data unintelligible; or o The measures taken subsequent to the breach ensure that the high risk to individuals is unlikely to materialize; or o Notification would involve disproportionate effort and public communication will be equally effective. • Requires notification of regulator and documentation
Low	• Breach of personal information that does not create a risk of harm • No notification but documentation

Content of notification:

- Nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned;
- Categories and approximate number of personal data records concerned;
- Likely consequences of the personal data breach;
- Measures taken or proposed to be taken to address the data breach;
- Name and contact details of the Data Protection Officer or other contact point.

Means of Notification:

- Directly and conspicuously by letter, email or telephone, as most effective; or
- Through public communication if direct, individual notification causes a disproportionate effort to what is necessary

TAB A INCIDENT REPORT

	INCIDENT REPORT NUMBER:
Date	
Time	
Location of breach	
Affected system(s)	
Affected data	
Containment measures	
Remediation measures	
Rationale for measures	
Follow up as necessary	
Resolution	
Date of resolution	

TAB B BREACH RESPONSE REPORT FORM

	BREACH REPORT NUMBER		
Date, Time and Location			
Affected Systems			
Affected Data			
Containment and remediation measures			
Breach Details			
Date & time of breach alert			
Date & time breach detection			
Date & time breach occurrence			
Place of Breach			
Name and title of person who detected breach			
How the breach was detected			
Type of breach	district m employee data	☐ Yes	☐ No
	district m client data	☐ Yes	☐ No

Part II – Containment

1. Breach Containment

.	Date & Time	Activities
Immediate steps		
Response Activities Report		

User (s) affected	Information / action requested	Due Date/Time	Status

Investigation

2. Breach investigation

Root cause of the breach (if known)	
Estimated number of individuals affected	
Assessed risk of harm to individuals	

Part V – Remediation and Prevention

Remediation	Date	Officer responsible	Progress	Completion Date

Report completion and approval

Report completed by:	Date
Report reviewed by:	Date
Report approved by:	Date

TAB C
NOTIFICATION REPORT

Information Involved

Risk Assessment	**Data breached**	**Example of data elements (e.g., name, credit card information)**	**Format of data**
	Non sensitive Description Sensitive Description	Click here to enter text.	☐ Encrypted ☐ Identifiable ☐ De-identified ☐ Pseudonomyzed

Text of Notification to Supervisory Authority:	
Date:	Follow-up:
Text of Notification to Individuals:	
Date:	Follow-up:

ANNEX D

GUIDANCE ON DATA PROTECTION CLAUSES FOR SERVICE AGREEMENTS – SUBJECT TO CLIENT NEGOTIATIONS

Introduction

This document does not constitute a template of district m's client agreements.

Included here are exclusively the contractual clauses relevant to **Personal Data Protection** district m commits to in the negotiation of Agreements in compliance with the General Data Protection Regulation (GDPR).

Security

district m is a Data Processor or Subprocessor for the Personal Data Processed on behalf of (CLIENT), which is a Data Controller or Processor, in the context of several contractual relationships, which are executed or will be executed with district m.

Provisions on data processing govern any processing of Personal Data undertaken by district m on behalf of (CLIENT) for the purpose of fulfilling the Agreements between district m and (CLIENT), which are already concluded and/or can be concluded in the future. district m shall process all Personal Data that it receives, possesses or otherwise obtains access to only for the purposes of the Agreements and in accordance with Applicable Data Protection Law and (CLIENT) instructions, as they may be issued from time to time.

Data Security. district m shall implement the security measures described in the Security and Infrastructure Guide. However you acknowledge that it is your responsibility to ensure that the set of security measures described thereunder meet your business needs. You further acknowledge that district m does not control and is not responsible for the transfer of data over telecommunications facilities, including the Internet. district m does not warrant secure operation of the Service or that it will be able to prevent third party disruptions. You agree that district m shall have no liability for:

(a) any provision of security-related services or advice that district m may voluntarily provide outside the scope of the Service specified herein; and

(b) for any security-related breach caused by you.

(c) the duration of the data processing strictly depends on the duration of the Agreement.

Data Protection. district m shall:

(a) Carry out processing of personal data supplied by you in the context of this Agreement strictly on your behalf and in accordance with the protection of technical and organisational measures in accordance with the Security and Infrastructure Guide;

(b) Process the personal data only on your documented instructions, including with regard to transfers of personal data to a sub-processor.

(c) Ensure that all persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, as described in the Security and Infrastructure Guide.

(d) Should it be necessary, assist you in responding to requests for exercising the data subject's rights under the GDPR;

(e) Make available to you all information necessary to demonstrate compliance with the obligations laid down in the GDPR as described in district m's GDPR Data Protection Framework. Should district m believe, however, that an instruction from you infringes the GDPR, we shall immediately inform you.

(f) Allow for and contribute to audits, including inspections, conducted by you or another auditor mandated by you.

In the event that district m should detect a data security incident or breach:

(g) it will notify you without undue delay in case of a breach;

(h) in case of an incident not resulting in a breach, it will notify you without undue delay if the incident is material to this Agreement.

district m shall immediately inform (CLIENT), in writing:

(i) of any public authority requesting disclosure of Personal Data;

(j) of any enquiries or requests from Data Subjects with respect to their Personal Data; and

(k) of any reasonably suspected or actual breach of security, loss or unauthorized use, disclosure, acquisition of or access to Personal Data (including hard copy records) or systems used for Processing Personal Data with

(i) in reasonable detail the effect on (CLIENT) if known, of the breach, loss or unauthorized use, disclosure, acquisition of, or access to, any Personal Data or systems used for Processing Personal Data and the corrective action taken or to be taken by district m;

(ii) district m shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with (CLIENT), in all reasonable and lawful efforts to investigate, prevent, mitigate or rectify such breach, loss or unauthorized use, disclosure, acquisition or access.

(CLIENT) and district m shall be separately responsible for conforming with such statutory Applicable Data Protection Law as is applicable to them. This applies in particular to the obligation to maintain a record of processing activities under our respective responsibility.

Return of Confidential Information and of Personal Information. Upon Disclosing Party's written request upon expiration or termination of this Agreement (or at any earlier time upon written requests by the Disclosing Party), the Receiving Party shall: (a) promptly deliver to the Disclosing Party all originals and copies, in whatever form or medium, of materials, in whatever form or medium, containing such Confidential Information in the Receiving Party's possession, power or control and the Receiving Party will delete all of the Disclosing Party's Confidential Information and Personal Information from any and all of the Receiving Party's computer systems, retrieval systems and databases; and (b) request that all persons to whom it has provided any of the Disclosing Party's Confidential Information and Personal Information comply with this section.

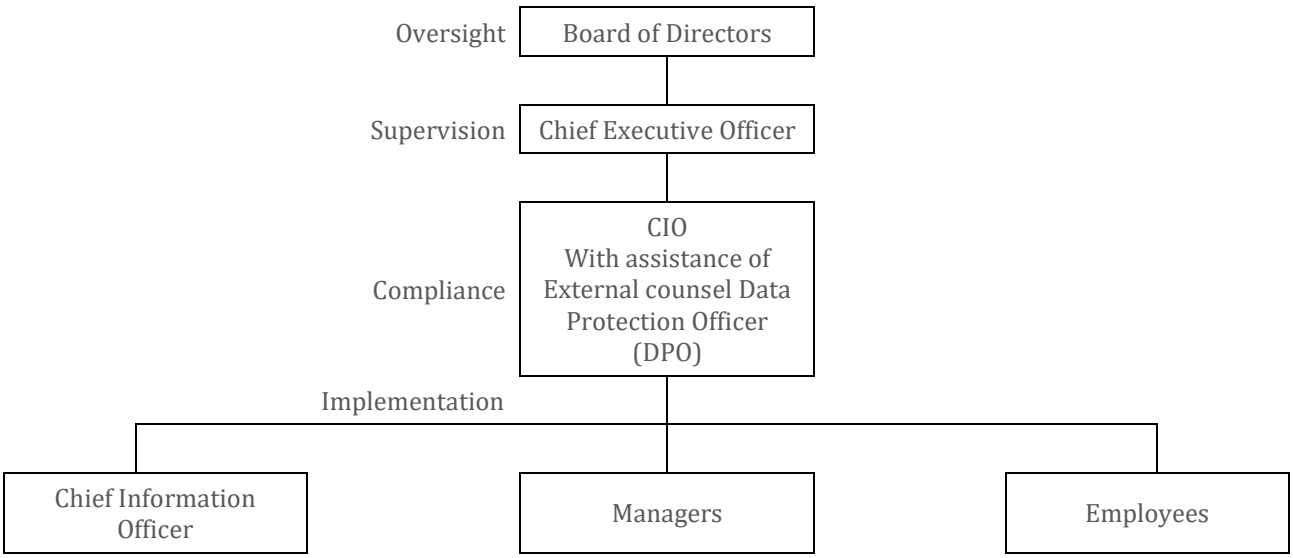
Use of Suppliers and Service Partners. You acknowledge that district m obtains certain services from third party providers (such as hosting partners, third party data storage centers or ISPs) and, as such, cannot control their performance or Service delays caused by them, other than what is provided for in the Service Level Agreement. However, district m shall at all times be responsible for the performance of its suppliers and service partners. district m's use of suppliers and service partners is governed by the following:

- district m shall be entitled to subcontract its obligations under this Agreement to third parties only with your written consent

- district m shall inform of any intended changes concerning the addition or replacement of other Sub-processors, thereby giving (CLIENT) the opportunity to object to such changes. If district m subcontracts its obligations under the Main Agreement with (CLIENT)'s prior written authorization, district m shall enter into a written agreement with the Sub-processor that will impose the same data protection and confidentiality obligations on the Sub-processor as are imposed on district m under this Agreement and in particular ensure that the Sub-processor implements the appropriate technical and organizational measures as required by the Applicable Data Protection Law and other statutory laws and regulations.

- Should district m subcontract its obligations under this Agreement to a subcontractor whereby your personal data is transferred to a country outside the EU not recognized as having adequate personal data protection, such contract will be subject to EU Standard Model clauses.

Data Protection Governance Framework



1. Compliance

External Counsel designated as Data Protection Officer (DPO)

While the General Data Protection Regulation (GDPR) only requires the designation of a DPO where the core activities of the controller or the processor require regular and systematic monitoring of data subjects on a large scale; or consist of processing on a large scale of special categories of data, district m has chosen to designate a DPO as a matter of good practice.

Chantal Bernier, Counsel, National Leader, Privacy and Cybersecurity Practice Group at Dentons Canada LLP is designated as DPO to district m with the following tasks:

As DPO, Chantal Bernier commits to the following tasks:

- Monitor compliance with obligations in relation to data protection according to the policies and processes district m has adopted in compliance of these obligations, including
  - the assignment of responsibilities to respond to individual requests and challenges to compliance,
  - awareness-raising and training of employees involved in processing operations, and the related audits,
  - consideration, in ensuring compliance, of the risk associated with processing operations, related to the nature, scope, context and purposes of processing.
- Inform and advise district m management and employees of their obligations in relation to data protection;
- Receive and respond to data protection information requests, individual access requests, rectification requests and complaints, as the case may be.
- In case of a breach, as described in district m's Incident and Breach Response Process,

- engage and coordinate the Core Breach Response Team upon detection of a breach, and the Full Breach Response Team, as necessary in accordance with the gravity of the breach as assessed by the CIO;
- advises the CEO, upon assessment of the gravity of the breach by the DIS, on notification of the breach
  - Addresses all requests from law enforcement authorities;
  - Acts as the contact point for the supervisory authority as necessary; and
  - Ensures confidentiality of DPO tasks.
  - As DPO to district m, Chantal Bernier may be reached at may be reached at chnatal.bernier@dentonsd.com

2. Implementation:

Chief Information Officer (CIO)

The CIO

- advises CEO on trends in security threats
- in case of a breach, as described in district m's Incident and Breach Response Process

- Leads the Core Breach Response Team in breach investigation and assessment
- Provides CEO assessment of nature, scope and gravity of the breach

Business line managers:

- ensure implementation of district m data protection policies and processes through staff supervision and training.

district m employees:

- endorse district m's data protection policies and processes and comply as a matter of professional duty and ethics;
- take on training to ensure full understanding of district m data protection obligations.

3. Supervision:

Chief Executive Officer (CEO)

- requires regular status reports on compliance;
- provides data protection compliance reports to the Board;
- decides on notification in the case of a breach, upon recommendation of the External Privacy Counsel
- with VP Finance & Administration, allocates resources to the DPO to carry out DPO tasks including ensuring compliance and responding to access and rectification requests or complaints

4. Oversight

Board members

- require regular status reports on data protection compliance from the CEO;
- hold senior management accountable for data protection;
- participate in data protection risk management should critical data at district m be threatened.

5. Liaison

Individuals, customers and supervisory authorities may communicate with:

- Chantal Bernier, the DPO, may be reached at chantal.bernier@dentons.com