# WORKING DRAFT

## A Plain Language Primer of Privacy Requirements for Use by Security Professionals

Draft date: January 11, 2021

### *INTRODUCTION*

In most aspects of the collection, use or processing of personal data, privacy and security functions overlap or coexist to some extent. To achieve their objectives and reduce risks to the organization in which their operate, information technology and information security professionals (IT/S Pros) and privacy professionals (Privacy Pros) should communicate regularly to ensure that their respective efforts complement, and do not conflict with, each other. Better communications will help improve their understanding of the ecosystem in which in which their organization uses or shares personal data, and make their activities more efficient and more effective.

#### *Purpose*

**This primer is intended to help bridge the communication gap between IT/S Pros and Privacy Pros. It provides a concise, plain English illustration of the objectives most commonly found in privacy laws around the world, and the context in which they arise, and explains the potential role of IT/S Pros in meeting those objectives.**

#### *Scope*

**This primer is not a compliance tool,** a checklist, a compilation of best practices, or other form of guidance. It is intended to be used to improve communications between IT/S and Privacy Pros, regardless of where they are located, or where their organization or its clients reside. This is possible because, at the highest level of abstraction, there are numerous similarities between most privacy laws, worldwide, because they derive from the same seminal documents, such as the 1980 OECD Privacy Guidelines, the first internationally agreed upon set of privacy principles.

#### *Definitions*

Because each country' law uses its own set of terms, we have attempted to use generic terms that can be easily understood, even if a specific country law use different terms. For example some countries call their law "data protection law" (e.g., Argentina, Brazil, Germany, or Qatar) whereas others call it "privacy law" (e.g., Canada, United States). We chose the shorter term "**privacy law**". Some laws refer to "personal data" (e.g., Switzerland, Uruguay or Spain), others use "personal information" (e.g., United States or South Africa). We chose the shorter term "**personal data**". Some laws refer to "data subject" (e.g., EU or South Africa), while others may use "data owner", "consumer", "child", "student", etc. We chose the term "**individual**".

***Organization***

This primer lists selected requirements found in most privacy laws where compliance with a particular requirement cannot be achieved without the tools, skills, knowledge or participation of IT/S Pros. For each requirement, there is a plain language description of the legal requirement, and the type of information, tools, features, or assurances that Privacy Pros are likely to need from their IT/S colleagues. These issues have been grouped in seven categories

1 – **General needs**: activities necessary to understand, at the high level, the nature of the data collected, how the data is used, and how it is shared

2 – **Specific legal requirements**: specific requirements, restrictions or pre-requisite to the collection and use of data, such as, data minimization, or the conduct of impact assessments

3 – **Oversight:** oversight and monitoring of the different participants (employees, contractors or service providers) to help ensure that they have a proper understanding of their obligations; and the precautions to be taken before engaging these participants

4 – **Data transfers**: awareness and implementation of restrictions to the transfer of personal data across borders

5 – **Security**: activities surrounding the provision of security, and response to a security incident as defined in data breach laws

6 – **Individuals rights**: identifying and responding to requests by individuals to exercise their rights under applicable law, such as right of access, right of erasure, or right to object to the use of data about them

7 – **Management**: role and obligations of management in ensuring compliance with the applicable personal data privacy laws.

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| **1- General needs** | **Categories of data being collected**<br>- General data<br>- Sensitive<br>- Children<br>- Technical | Ensuring that the entity provides adequate security levels that are adapted to the specific nature, sensitivity, risks, or legal requirements that apply to the different categories of personal data that the entity handles (e.g., processes, uses, stores, transfers or shares with others).<br><br>Ensuring that IT/S is aware of the different categories of data to be collected and processed, and keeping them informed when changes occur. | - *Understand the nature and different types of data to be processed, and make available the required or recommended tools and controls that are adapted to each category of personal data.*<br>- *Keep informed of the changes in legal and other requirements over time concerning the protection of the data.*<br>- *Design and apply the processes and tools necessary to achieve the goals.*<br>- *Communicate the existence of these tools, and as applicable, their limitations to the Privacy Pros.*<br>- *Update the tools as needed, and communicate the changes. If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **1- General needs** | **Special categories of data**<br>for example, depending on applicable law<br>- Children data<br>- Location data<br>- Health data | Laws that govern the protection of personal data often identify special categories of data that require special scrutiny, for example prior permission or additional security measures. In this context, the Privacy group might be responsible for:<br><br>Ensuring that the IT/S function is aware that certain types of data that are deemed | - *Understand the nature and different types of special categories of data to be processed, and make available the required or recommended tools and controls that are adapted to each category of personal data.*<br>- *Keep informed of the changes in legal and other requirements over time* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | - Information about religion or other beliefs<br>- Information about membership in trade association<br>- Genetic data<br>- Financial of credit data | "special category of data" under the applicable law may be collected.<br><br>Ensuring that specific measures as dictated by the applicable privacy law(s) are in place. | *concerning the protection of the special categories of data, as applicable.*<br>- *Design and apply the processes and tools necessary to achieve the goals.*<br>- *Communicate the existence of these tools, and as applicable, their limitations to the Privacy Pros.*<br>- *Update the tools as needed, and communicate the changes.*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **1- General needs** | **How data is collected**<br>- Directly provided by individual<br>- Automatically collected (Website)<br>- Obtained from third party sources;<br>- Operations, maintenance, support, . . . | Ensuring the authenticity and the reliability of the sources of the data.<br><br>Ensuring that the means used to collect the data (from the individual, outside sources, applications, etc.) are appropriate to ensure data quality and authenticity. | - *Cooperate in the design of the tools used to collect data and ensure data quality, reliability, etc. as needed to meet the specific requirements of the proposed uses of the data (e.g. difference between data that will be used for sensitive purposes or for a long duration, and data that is used for counting the number of visitors to a website at a particular time of the day).*<br>- *Apply the processes and tools necessary to achieve the goals.*<br>- *Communicate the existence of these tools, and as applicable, their limitations to the Privacy Pros.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | - *Update the tools as needed, and communicate the changes.*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **1- General needs** | **How and for what purpose the data is used**<br>- Different types of security measures may be needed to ensure the security of the personal data during each of the processing activities<br>- These security measures may need to be updated | Ensuring that the appropriate security measures that are adapted to the specific uses of the personal data are available and are used during each of the processing activities.<br><br>Ensuring ongoing availability and efficiency of these measures.<br><br>Ensuring that these measures are adequate and adapted to the functions being conducted, including new, additional functions.<br><br>Ensuring that the measures are updated as needed to take into account changes in uses, technologies or applications, laws, etc. | - *Keep up-to-date regarding the changes in the use of the personal data*<br>- *Keep informed of the changes in specifications, features, needs, requirements of the different applications used to process personal data, their effect on the different categories of personal data, in order to adapt the security measures accordingly.*<br>- *Adapt its processes and tools as necessary to achieve the security goals and keep up with changes in threats, attacks, etc.*<br>- *Participate in keeping and updating records of processing.* |
| **1- General needs** | **Location**<br>- Where is the individual located | Determining which law applies, and where the affected individuals and their personal data are located. | *Data Location is a sensitive issue that touches on several areas. Privacy Pros need to know where data is located, and to be informed if the* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | - Where is the personal data located | The location of the organization, location of the individuals concerned and location of the personal data to be processed are critical information needed to determine which privacy law(s) may apply.<br><br>Further, several privacy laws contain unique prohibitions or requirements that relate directly to the country where the individual is located, and where the personal data is processed or might be transferred.<br><br>Key information needed to be able to process with a project, and maintain compliance on an on-going basis includes:<br>- Knowing which privacy law(s) apply<br>- Whether there might be requirements on data localization<br>- Whether there might be restrictions on transfers of data to another country | *location changes. IT/S Pros are likely to have direct, up-to-date knowledge of*<br>- *The location of the individuals with whom the organization interacts;*<br>- *The location of the personal data processed, e.g. where the data originated, where it is stored, processed, or might be transferred*<br><br>*Thus IT/S Pros should*<br>- *Provide Privacy Pros with up-to-date information about the location of servers, back-up servers, disaster recovery locations, archive servers, and where personal data are stored or processed*<br>- *Keep track of proposed movement of data, and inform the Privacy Pros of these changes ahead of time to avoid making changes that might cause a violation of data location laws.*<br>- *Be prepared to share documentation regarding its processes and the choices made regarding data location, to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| | | | - |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| **2- Specific requirements** | **Data Protection by Design and by Default; or Privacy by Design and by Default** | Some Privacy Laws may specifically require the development of, and compliance with, responsible practices that ensure privacy of all personal data of affected individuals at all stages of the life cycle of a product or service. The term used in the laws (e.g. under GDPR) or in white papers or reports (e.g. report issued by Federal Trade Commission in the United States or report of the supervisory authority in Canada). These laws or best practices require or urge companies to develop and abide by clear and practical "Data Protection by Design and by Default Principles (DPbDD)."<br><br>Ensuring that the applications used to process personal data are developed in accordance with DPbDD Principles<br><br>Monitoring compliance with these DPbDD principles throughout the life of the application and use of the personal data<br><br>DPbDD is the term used in the EU's GDPR, other laws or standards may use a variant, for example in Canada, the term originally used was "Privacy by Design" or "PbD") | - *Participate in the development of the DPbDD Principles*<br>- *Explain to the Privacy Pros the security implications that might be associated with compliance with each DPbDD principle*<br>- *Communicate and interact with Privacy Pros to understand their approach when developing their apps, products, services, and internal apps with the goal of following the DPbDD principles*<br>- *If requested, document its processes and the choices made when meeting their DPbDD obligations, in order to help Privacy Pros meet their Accountability Obligations under applicable Privacy laws.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| **2- Specific requirements** | **Data minimization**<br>- Data privacy laws require that the entity collect and use the minimum amount of personal data.<br>- Security may need to rely on large amount of data to identify patterns, anomalies, etc. that in turn may be used to identify a security incident | Ensuring compliance with data minimization requirements, i.e. collecting the minimum amount of data necessary to accomplish the purpose for which the data is being collected. The needs and criteria may be different from one function to another.<br><br>As part of its accountability obligation, ensuring and being able to document that all forms of personal data processing conducted by the organization - including the security function - use only the smallest amount of personal data reasonably necessary for that purpose, and retain such amount of data only for the shortest duration. | - *Explain the nature and amount of data needed to conduct certain functions, such as the detection of patterns of suspicious uses or processing.*<br>- *Show how each Security function complies with the data minimization principle.*<br>- *Explain why you decided that the amount of data collected was the minimum necessary to provide the optimum level of security under the circumstances.*<br>- *If necessary modify the processes and procedures to ensure better data minimization.*<br>- *If requested, document the processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **2- Specific requirements** | **Data Protection Impact Assessment (DPIA)**<br>- When the entity conducts a DPIA in connection with a proposed new use of the data, or a new product or | The purpose of a DPIA is primarily to evaluate the feasibility, risks, consequences from a privacy standpoint of a proposed collection, use, new use personal data.<br><br>Among other things some of those risks and questions involve IT/ Security issues, including some that the Privacy Pros might not be able to identify or anticipate. | - *Participate in the different stages of the DPIA Process, including, for example, to explain the likely consequences or obstacles that may arise when trying to provide adequate security for the new contemplated uses.*<br>- *Identify whether and how, and at what cost, it will provide the security required* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | service that involves new personal data or a new use of personal data | Thus a DPIA cannot be conducted in a privacy silo, and some of the activities associated with the preparation of a DPIA usually include:<br><br>Ensuring that the entity has identified the potential security risks and has in place (or can provide) the specific safeguards, security controls and mechanisms that are appropriate and adapted to the security risks that might result from the potential processing, in the specific circumstances described in the DPIA. | *by the new contemplated use, and the related obstacles, costs, etc.*<br>- *Commit to provide the security levels adapted to the new uses, if any, when needed.* |
| **2- Specific requirements** | **Identity verification**<br>- Identity of the individual or entity providing the data<br>- Identity of the individual or entity accessing the data<br>- Identity of the individual making a request (request for access, | Ensuring that the entity has in place the applicable mechanisms to enable verification of the identity of the individuals who provide data, or seek access to data, or the quality of the source of the data. | - *Understand the needs for identity verification, in which circumstance it is needed, the purposes, the turn-around time, etc.*<br>- *Participate in the design of the identity verification templates for the different circumstances where identity verification is needed.*<br>- *Apply the processes and tools necessary to achieve the identification and other goals, as needed, and ensure that they work.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | request for deletion, etc.)<br>- Identity of the individual providing consent<br>- Identity of the individual providing the explicit consent (double opt-in) | | - *Be aware of the applicable turn-around times that may be imposed by applicable laws.*<br>- *If requested, document the processes used, and the choices and trade-offs made.* |
| **2- Specific requirements** | **Data retention** | Ensuring that personal data is retained only as necessary or that the personal data is de-identified, anonymized or encrypted | - *Participate in the design of the entity's data retention policy*<br>- *Provide the appropriate processes and tools to ensure proper compliance with data retention policy*<br>- *Monitor data disposal processes at the end of the retention period.*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **2- Specific requirements** | **Data disposal** | Ensuring that the entity is able to dispose of the data in a way that complies with applicable laws and best practices | - *Communicate the security risks associated with data disposal.*<br>- *Discuss alternative means, and their adequacy for the particular circumstances.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | - *Provide procedures and tools for secure data erasure / disposal*<br>- *Keep up-to-date and share a data disposal policy.*<br>- *Have in place the safeguards and controls necessary to ensure compliance with data disposal policy.* |
| **2- Specific requirements** | **Records of processing and other filing requirements** | Ensuring that compliance documents required by law contain complete and accurate information.<br><br>Numerous data privacy laws (for example GDPR, Art. 30) require that the entity prepare written reports of its activities. Some of these reports, such as the "Record of Processing" under GDPR and national laws derived from GDPR, must be kept internally and provided to upon request to an authorized party (for example to a data supervisory authority.<br><br>In other cases, an entity may be required to file a document with detailed information on its collection, use, sharing, protection measures, etc. with the applicable data supervisory authority. | *On an ongoing basis*<br>- *Cooperate with the Privacy Pros in collecting and providing to the relevant party (likely to be Privacy or Compliance Professional ) the required documentation in a timely manner.*<br>- *Ensuring that the information above is complete, accurate, relevant and up-to-date*<br>- *Keeping track of changes to the entity's operations that may affect the content of the report.*<br>- *If the report reveals potential problems, take appropriate actions and notify management as applicable.* |
| | | | |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| **3- Oversight** | **Access by Employees and Third Parties**<br>- When employees (or contractors, consultants), or third parties (service providers, business partners) have access to data | Ensuring that access to data is limited according to roles and responsibilities identified in the entity's data processing policies<br><br>Ensuring that each recipient of personal data has appropriate security controls in place (e.g. through contracts, DPAs, or by performing due diligence).<br><br>Ensuring that appropriate contracts (e.g. data processing agreement, confidentiality agreement, services agreement, etc.) are in place with all those who have access to the personal data, e.g. subprocessors. | *On an on-going basis, coordinate with Privacy Pros to:*<br>- *Establish and negotiate the terms of the contracts needed to engage employees, consultants, service providers that may have access to personal data*<br>- *Ensure that proper assistance regarding applicable security measures is provided; e.g. explanation, clarification, awareness*<br>- *Monitor and oversee the employees, third parties, subprocessors, etc. to ensure compliance with the security measures laid out in these contracts*<br>- *Coordinate with Privacy Pros if updates to these contracts are necessary*<br>- *Be prepared to share documentation regarding IT/ Security processes and procedures to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **3- Oversight** | **When engaging subprocessors, or contracting with third parties** | Conducting appropriate due diligence when considering a new subprocessor or a new relationship with a third party that might gain access to the data.<br><br>Ensuring that the subprocessors have – and continue to maintain – adequate security | - *Conduct security due diligence of proposed subcontractor, subprocessor or third party*<br>- *Conduct periodic security audits as needed.*<br>- *If requested, document its processes and the choices made to help Privacy* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | measures that meet the contractual provision.<br><br>For that purpose, conducting due diligence and periodic audits. | *Pros meet their Accountability Obligations under applicable laws.*<br>- *Provide the identity of the third parties, consultants, service providers, etc. who have access to personal data as part of their IT/S function. These disclosures might be required by applicable laws*<br>- *Conduct period updates of the due diligence, and provide updates of the above reports.* |
| **3- Oversight** | **Training** | Ensuring that those who have access to personal data have received appropriate training with respect to the applicable laws, their obligations under those laws, or as identified in contracts, and or laid down in the entity's policies. | *On an on-going basis, coordinate with Privacy Pros to:*<br>- *Participate in the design of training course*<br>- *Ensure that security personnel have proper training in privacy matters*<br>- *Ensure that privacy personnel have proper training in security matters*<br>- *Participate in table top and other exercises to test the efficiency of the training.*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| | | | |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| **4- Data Transfers** | **Transfer of personal data to or from the organization** | Reducing the risks that any transfer of personal to or from the organization, or within the organization cause a violation of applicable laws, contracts, standards or policies.<br><br>For these purposes rules should be established after the risks have been identified.<br><br>This is likely to require the cooperation of several departments of the organization, such as legal, compliance, privacy, security, IT. | *IT/S Pros should be prepared to*<br>- *Participate in the development of policies and procedures related to the movement of personal data in, out and within the organization in cooperation with Privacy Pros and other departments.*<br>- *Provide up-to-date information about the location of data, servers, back-up servers, disaster recovery systems, archives, storage, as well as mobile or portable devices*<br>- *Provide period updates to the information above*<br>- |
| **4- Data Transfers** | **Crossborder data transfers: If data is to be transferred across borders, or processed in third countries** | Ensuring that attempts to transfer data across borders outside a region that restricts data transfers to certain categories of countries are immediately identified.<br><br>Ensuring that, as applicable, any such attempted transfers is allowed, blocked or modified in accordance with the policies, contracts, and legal obligations of the organization.<br><br>Preparing documentation, contracts, policies that address the restrictions to crossborder data transfers. | - *Provide up-to-date information about the location of servers, back-up servers, disaster recovery locations, archive servers.*<br>- *Keep track of server location, data location and proposed movement of data, to limit errors that could lead to violation of data transfer laws.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | |
| | | | |
| **5- Security** | **Security measures** | Ensuring that the specific security measures required by applicable laws, and those security measures identified in the applicable DPIA, if any, are in effect. For example,<br><br>Under HIPAA, for example:<br>- Special requirements for data in storage<br>- Special requirements for data in transit<br><br>Under Data Deletion or Disposal Laws, for example:<br>- Special requirements when hiring a service provider<br><br>Under GDPR, for example, the entity should have in place, to the extent possible:<br>- Means to pseudonymize personal data<br>- Means to encrypt personal data<br>- Means to ensure the ongoing confidentiality of processing systems and services | - *Communicate with Privacy Pros when identifying the risks to the data and evaluate the likelihood of such risks in view the potential uses of the data in order to develop a reasonable and adequate risk-based approach*<br>- *Ensure that the security measures being developed and used meet the Data Protection by Design and by Default (DPbDD) policies established by the entity, and the necessary measures identified in previously developed DPIA.*<br>- *Some Privacy Laws may impose unique security requirements that apply only to certain types of personal data; ensure that complete information is provided by Privacy Pros, for example, there might be unique requirements under Financial Services laws that address data privacy.*<br>- *While all security functions are fully under the IT/S group, the IT/S group may have to change or update its practices. IT/S Pros should periodically communicate with the Privacy Pros to ensure that these proposed changes or updates are not likely to conflict with* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | - Means to ensure the ongoing integrity of processing systems and services<br>- Means to ensure the ongoing availability of processing systems and services<br>- Means to ensure the ongoing resilience of processing systems and services<br>- Means to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident<br>- Process for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures for ensuring the security of the processing.<br><br>And if such is not possible, being able to demonstrate why these security tools or methods are not used | *the Privacy laws with which the organization must comply.*<br>- *If requested, document the processes and choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **5- Security** | **Data Breach Preparedness** | Most privacy or data protection laws require organization to notify government agencies, data protection authorities, individuals, etc. when a "personal data breach" occurs. | *A Data Breach Response Plan touches on a wide variety of issues. Among those issues, there are numerous IT/S issues, which the IT/S Pros are better able to address.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | While definitions vary from one law to another a "personal data breach" is usually defined as a breach of security that results in unauthorized access to personal data, loss of personal data, making personal data inaccessible, etc. in such a manner as potentially causing harm to one or more individuals.<br><br>When such an incident occurs, an organization must conduct a series of activities within a short timeframe. It is often a legal requirement (or at a minimum a prudent practice) for organizations to develop an "incident response plan" that specifies what to do when a security incident appears to be a "personal data breach".<br><br>Privacy Pros are frequently responsible for developing a "Data Breach Response Plan," an Incident Response Plan that addresses the unique issues related to a "personal data breach" and that meets the requirements of the applicable privacy laws.<br><br>In addition, applicable laws in this regard, frequently require that formal training on the application of the Data Breach Response Plan be conducted. | *The team that is tasked with the preparation of the Data Breach Response Plan is likely to seek assistance from the IT/S Pros for some chapters of their Plan. Thus IT/S Pros should:*<br><br>- *Be prepared to work with the team tasked with the preparation and testing of the Data Breach Response Plan;*<br>- *Keep in mind that some of the requirements or obligations to be included in the Plan - for example turn-around time- may be dictated by applicable privacy or data protection laws;*<br>- *The Plan will need to be re-evaluated from time to time, and updated as laws change, and as the practices of the IT/S group - or other departments within the organization - change;*<br>- *There is a significant legal risk in failing to design and adopt a proper Data Breach Response Plan*<br>- *Participate in training the personnel in the details of the Data Breach Response Plan, such as in the form of technical or practical session, or by conducting "fire drills" or "table top exercises"* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| **5- Security** | **Data Breach Response** | Ensuring that, in the event of a security incident, the entity will be able to perform in accordance with the Data Breach Response Plan prepared per the section above.<br><br>Whether or not a Data Breach Response Plan exists, in the event of a security incident, the organization must promptly conduct, and an expedited manner, the activities necessary to address its compliance obligations in this regard, such as:<br><br>- Identify nature and scope of the incident<br>- Determine whether the incident is a "personal data breach" as defined by applicable laws<br>- Determine whether it is a reportable data breach, as defined by applicable laws<br>- Provide the broad range of information required to be provided when notifying the occurrence of a data breach, as defined by applicable law. | *When a security incident occurs:*<br>- *Cooperate with the Privacy Pros in evaluating the incident and determining whether the incident is a "data breach" as defined in the applicable Privacy law or laws.*<br>- *When a "data breach" has been identified, cooperate with the Privacy Pros in evaluating whether the "data breach" is a "reportable data breach", as defined in the applicable Privacy Law or Laws.*<br>- *Keep in mind that the definition of what constitutes a "reportable data breach" varies from one law to the other.*<br>- *Identify and apply promptly the necessary measures to mitigate the effect of the data breach. Note that this is a security function, but keep proper records as directed by the Privacy Pros because they may need those records.*<br>- *Participate in the preparation of the documents, descriptions, and breach notices required by applicable privacy law(s) within the time frames identified in these laws.*<br>- *Participate in the preparation of press releases, communiqués, and other notices identified in the entity's Data Breach Response Plan* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | - *Be prepared to provide written documentation of the organization's activities under the purview of the IT/S Pros because it may requested by the Privacy Pros to meet their Accountability Obligations under applicable laws.* |
| **5- Security** | **Business Continuity Emergencies other than Data Breaches Work-from-home** | Ensuring that the business has in place the proper functions, tools, policies, to allow the continuity of the operations in case of a technical or physical disaster such as loss of power, loss of climatization, strikes, fire, etc., such as:<br>- relocation of data to a different server or location<br>- relocation of personnel to a different location<br><br>Ensuring that personal data of employees and customers are protected when working outside of usual circumstances. | - *Educate the Privacy Pros about the unique security issues that may arise in case of a physical or technical disaster*<br>- *Cooperate in establishing a disaster recovery plan that takes into account the constraints created by privacy or privacy laws in the event of an emergency.*<br>- *Interact, cooperate and communicate with Privacy Pros, in the event of an emergency to develop a common approach that ensures that both personal data and entity data are protected.*<br>- *With the change in work conditions resulting from the pandemic similar issues may arise. Coordinate as needed with the Privacy Pros to adapt the pre-existing documents and policies to the new turn of events, as necessary.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | |
| **6- Individuals' rights** | **Individuals' rights (in general)** | Ensuring that there are in place means to receive the individual's requests, and authenticate the individual making the request<br><br>Documenting that the authentication or verification procedure has been performed. | - *Most privacy laws grant individuals a number of rights and allow individuals to contact an entity to exercise those rights.*<br>- *Because of the sensitivity of the information sought, or to be changed or erased, security plays an important role.*<br>- *Thus, IT/S should be prepared to participate in the different stages of the process, such as design of the templates used to communicate with an individual, the type of data needed to authenticate the individual, the activities that result from the request, etc.*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **6- Individuals' rights** | **Right to be Informed** | Ensuring that the organization informs the individuals of their right (if any) to be informed about the collection and use of their personal data when the data is obtained, and that the data may be available only for a specific period of time. | - *Keep informed of the needs of the business for information that might be deemed "personal data" (or equivalent)*<br>- *Help communicate the technical reality to the consumer or end user with the proper level of detail and clarity*<br>- *Pay particular attention to communications with parents or* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | *guardians with respect to children's personal data*<br>- *Be prepared to respond to a request for information concerning the collection and processing of personal data* |
| **6- Individuals' rights** | **Request for Access** | Ensuring that the entity is able to respond, in a secure way, to a Request for Access: e.g.,<br>- Verify the request and the identity of the individual making the request;<br>- Receive and record the request;<br>- Collect and prepare a copy the data that meet the requirements;<br>- Identify potential obstacles to providing the requested access (e.g. if personal data is combined with another person's data).<br><br>Documenting the response to the request for access. | - *Cooperate with Privacy Pros in designing and maintaining the features, applications and records necessary to receive, register and respond to a request for access to personal data. For example:*<br>- *As applicable, participate in the receipt and recording of the requests for access to personal data*<br>- *Verify the authenticity and legitimacy of request, and of the identity of the requesting person*<br>- *Determine (in cooperation with the Privacy Pros) which personal data has been collected, including assess the complexity and costs of the collection, identification of the relevant forms of data that might respond to the request*<br>- *Assist in the collection of the requested information while maintaining adequate security of that information, and other information (e.g. personal or confidential data that pertains to third* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | *parties and that might create a risk to third parties)*<br>- *Cooperate with Privacy Pros in identifying the information that responds to the requests,*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **6- Individuals' rights** | **Request for Correction** | Ensuring that the entity is able to respond, in a secure way, to an individual's Request for Correction; e.g.<br>- Verify the request and the identity of the individual making the request;<br>- Determine whether the request is founded;<br>- Evaluate and anticipate effects of the correction on the efficacy or strength of pre-existing security measures;<br>- Evaluate the effect of the correction on third parties or service providers, such as the need to inform certain third parties or service providers about the correction, or requiring them to also make the correction, if applicable; | - *Cooperate with Privacy Pros in designing and maintaining the features, applications and records necessary to receive, register and respond to a request for correction of personal data. For example:*<br>- *As applicable, participate in the receipt and recording of the requests for correction*<br>- *Determine (in cooperation with the Privacy Pros) whether the request for correction is founded, and how to respond to it.*<br>- *Identifying which personal data must be corrected, and how the correction may be made in a secure manner; including assessing the complexity and costs of the correction.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | - Meet the time frames and other requirements identified in applicable laws.<br><br>Communicating to third parties, or service providers the need to complete the correction in their databases as required by applicable laws.<br><br>Documenting the response to the Request for Correction | - *Once the corrections are made, determining how to disseminate among third parties, service providers, etc. the need to make the corrections in a safe and secure mode*<br>- *Assess the complexity and costs of the collection, and identifying the restrictions, exceptions and other barriers to the corrections*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.*<br>- |
| **6- Individuals' rights** | **Request for deletion, blocking, restriction of the processing, objection to the use of personal data** | Ensuring that the entity is able to respond, in a secure way, to an individual's request for deletion, blocking, restriction of processing or objection to the processing; e.g.,<br>- Ability to verify the validity of the request, and the identity of the individual allegedly making the request,<br>- Existence of a process for receiving and recording the request;<br>- Ability to determine whether the request is founded or whether there are exceptions, exemptions,<br>- Identifying the potential effects of the deletion, blocking or restriction of | - *Cooperate with Privacy Pros in designing and maintaining the features, applications and records necessary to receive, register and respond to a request for deletion, blocking, restriction of the processing. For example:*<br>- *As applicable, participate in the receipt and recording of the requests for deletion, blocking, restriction of the processing*<br>- *Determine (in cooperation with the Privacy Pros) whether the request for deletion, blocking or restriction of processing meets the requirements in* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | the processing on third parties or service providers, such as the need to inform certain third parties or service providers that the data has been deleted, blocked, or its processing restricted<br>- Requiring such third parties or service providers to delete, block or restrict the processing, as applicable<br>- Evaluate the effects of the deletion, blocking, restriction, on the security measures used by the entity or by its service providers or others<br>- Meet the time frames and other requirements defined in applicable laws.<br><br>Ensuring that, if data is to be deleted, the data disposal is completed in compliance with the relevant data disposal or deletion laws.<br><br>Communicating to third parties or service providers the request for deletion, in accordance with applicable law.<br><br>Documenting the response to the request for deletion, blocking, or restriction of the processing. | *the applicable laws, and how to implement such request.*<br>- *Identifying which personal data must be delete, blocked, restricted, and which may not or must not the deleted, blocked, restricted, due to legal, contractual or other requirements*<br>- *Identifying how the deletion, blocking, etc. may be made in a secure manner; including assessing the complexity and costs of the correction.*<br>- *Once the deletion, blocking, or restrictions have been completed, conduct the applicable reporting, archiving, etc. required by laws, regulations, policies, etc.*<br>- *Assess the complexity and costs of the collection, and identifying the restrictions, exceptions and other barriers to those activities*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| **6- Individuals' rights** | **Request for data portability** | Ensuring that the entity is able to respond, in a secure way, to an individual's request for portability; e.g.<br>- Ability to verify the validity of the request, and the identity of the individual allegedly making the request;<br>- Establishing a process for receiving and recording the requests<br>- Determining whether there are exceptions, exemptions, obstacles, prohibitions, etc.<br>-<br>- Determining whether there are technical, physical or legal obstacles to collecting and organizing the data in preparation for the transfer;<br>- Determining whether there might be security obstacles to the collection or transfer of the data<br>- Identifying the means to be used to transfer the requested data in a secure way;<br>- Complying with the time frames and other requirements defined in applicable laws.<br><br>Documenting the response to the request for portability | - *Cooperate with Privacy Pros in designing and maintaining the processes, specifications, applications and records necessary to receive, register and respond to a request for data portability. For example:*<br>- *As applicable, participate in the receipt and recording of the requests for portability, and identifying all records to be transferred and records that should not be transferred.*<br>- *Assess the complexity and costs of the collection, and identify the restrictions, exceptions and other barriers to those activities.*<br>- *Determine (in cooperation with the Privacy Pros) whether the request for data portability meets the requirements or definitions in the applicable laws, and how to implement such request.*<br>- *Identifying which personal data must be transferred, and which may not or must not be transferred.*<br>- *Identify the consequences of the transfer (and likely subsequent deletion or blocking of the data) on the efficacy of the overall security of the entity's databases;* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | - *Determine the related measures, such as whether data must be (or not be) archived, or must be (or not be) erased.*<br>- *Identifying how the deletion, blocking, etc. may be made in a secure manner; including assessing the complexity and costs of the correction.*<br>- *Once the transfer is completed, conduct the applicable reporting, record keeping, archiving, etc. required by laws, regulations, policies, etc.*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| **6- Individuals' rights** | **Rights concerning Automated Processing & Profiling** | Ensuring that the entity is able to respond to an individual's request regarding automated decision making and provide explanations on the logic used.<br><br>Verifying the identity of the individual making the request, and the nature and scope of the request<br><br>Communicating internally with the stakeholders to provide response within the time frames, and in the form, required by applicable law. | - *Cooperate with Privacy Pros and others in designing and maintaining the features, applications and records necessary to receive, register and respond to a request for regarding profiling: For example:*<br>- *As applicable, participate in the receipt and recording of the requests for information regarding profiling and similar activities*<br>- *Determine (in cooperation with the Privacy Pros) whether the request meets* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | Documenting its response to the request concerning automated processing and profiling. | *the requirements in the applicable laws, and how to implement such request.*<br>- *Identifying which information to be provided.*<br>- *Once the issue addressed conduct the applicable reporting, archiving, etc. required by laws, regulations, policies, etc.*<br>- *Assess the complexity and costs of a change in the methods previously used, to avoid encountering similar problems or other barriers to those activities*<br>- *If requested, document its processes and the choices made to help Privacy Pros meet their Accountability Obligations under applicable laws.* |
| | | | |
| **7- Management** | **Oversight and monitoring** | Ensuring that when Privacy Group conducts its monitoring and audit activities, it receives adequate assistance and cooperation from IT/ Security Group | - *IT/S is likely to be requested to have processes and tools available to provide the assistance needed.* |
| **7- Management** | **Assistance and Cooperation** | Ensuring that the respective leaders of the Privacy Group and the IT/S Group conduct periodic meeting to coordinate activities, findings, concerns, and proposed changes | - *These activities require full cooperation and interaction of the Privacy Group and the IT/S group*<br>- *Time for regular meetings should be allocated.* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | | - *Both sides should share the names and contact information of the individuals, and as applicable identify other individuals, and should promptly inform each other of changes in leadership or participants* |
| **8- Management** | **Accountability; Record Keeping**<br>- Most laws and data supervisory authorities require that organizations be able to document how they comply with the applicable privacy or data protection laws. | Ensuring that the organization keeps appropriate records of its activities so that it can demonstrate:<br>- That it complies with the requirements of applicable privacy or data protection laws and principles,<br>- That is has in place measures that are appropriate, adequate and effective for the intended purposes.<br>- That it has conducted proper evaluation of the needs and the risks in order to identify the measures and means that are the appropriate to address the requirements of the applicable privacy and data protection laws within the framework of its operations, its budget, workforce, the nature, sensitivity and volume of personal data to be processed, the nature of the processing, and the risk associated with this processing | - *IT/S is likely to be requested to:*<br>- *Participate in the development of some of these processes, procedures, etc.*<br>- *Implement these processes, procedures, at a minimum in those of its operations that pertain to the processing of personal data*<br>- *Have in place processes and tools available to provide the assistance needed.*<br>- *Keep, and when so requested, be able and willing to provide, documentation regarding its processes and the choices made, and the training provided to its personnel on those policies, processes, etc.,* |

| *Privacy Law Requirement; Goals and Information Needed* | | | *Potential Role of IT/S Pros* |
|---|---|---|---|
| | | Ensuring that the company can demonstrate that it complies with the rules, policies, procedures, or processes that it has chosen to meet its obligations, and that it keeps its personnel informed and trained on these rules, policies, etc.<br><br>Ensuring that the company keeps an appropriate record of processing activities that meet the applicable legal requirements or industry best practices. | |