



Re: **Attestation regarding Informatica privacy practices mapped to PbD for the purpose of being recognized as an Organizational PbD Ambassador.**

As a champion of data security and privacy best practices, Informatica Corporation (www.SecurityandPrivacy.ca) strives to not only educate clients, offer high quality consulting and deliver advanced solutions that address information risk, but also to consistently demonstrate a high degree of adherence to privacy principles.

This is evident in the way our company handles personal information, enforces data protection policies and educates staff on responsible use of sensitive data. This high standard is exemplified by a passion to lead by example and continues to deliver unique opportunities.

How Informatica Demonstrates Adherence to the 7 Foundational PbD Principles

1. *Proactive* not Reactive; *Preventative* not Remedial

To prevent security and privacy breaches, the organization must have a thorough understanding of preventative controls. **The key confidentiality control in consistent use by Informatica is the pervasive use of data encryption** for sensitive data. From encrypting personal information, financial transactions, health details, client data and access credentials to ensuring that clients adopt a convenient method and make it a part of their daily operations, Informatica is an avid proponent of data encryption when it is absolutely imperative that breaches be prevented, rather than merely 'addressed'.

2. Privacy as the *Default Setting*

One of the key aspects of data protection at Informatica is the enforcement of data integrity controls. Controls such as access logs, activity monitoring and most of all, data integrity protection are an integral part of Informatica's '**security by example**' approach. This dimension of security monitoring ensures that data can be verifiably trusted at all times and complements existing **fundamental controls** that make up the organization's protective envelope.

3. Privacy *Embedded* into Design

Informatica believes that security and privacy **must not only be pervasive, but also effortless**. As such, internal controls are designed, developed and embedded into processes that are prototyped internally and thoroughly tested before being recommended to clients. Our seamless and effective internal controls are modular enough to package and assist clients in

implementing such as in the cases of executive advisory services (**FlexProtect Risk Advisor™**), risk assessments (**FlexSecure Verify™**), **WorkLife™** Security & Privacy Education and **FlexProtect SPM™** Project Management. The first two reflect our own internal controls, while the latter two are as much commercial solutions as internal ones, since we perfect and employ the same project management and education principles internally, before ever recommending them to clients.

4. Full Functionality — *Positive-Sum*, not Zero-Sum

One of the first descriptive statements Informatica makes about its services is that they're based on a 'proprietary methodology'. This means – in part - that the protective controls embedded into every service we provide are repeatable and scalable. Every process step, access control and security measure we build into our solutions is designed to be unobtrusive and easily adopted by our clients (at the relationship level) and interlocutors (in the case of data communications). By seeking to have a deep understanding of client constraints, we are further able to ensure a high degree of continuity, equivalence and harmony between our own internal controls and those of the parties we interface with, with no adverse effect on performance, relationship or functionality. In fact, we are able to communicate all the requirements we enforce for the protection of data in a positive light, and that is always met with respect and acquiescence by third parties, precisely because **we insist on positive sum outcomes**.

5. End-to-End Security — *Full Lifecycle Protection*

One of the very first concepts we present in our internal staff training on Security and Privacy Awareness is the concept of '**information as a life form**'. When treated as an indispensable, fluid substance, information comes to life in the audience's mind. From an abstract concept to a concrete, living entity, information is created, accumulated, replicated, stored, transferred and it ultimately expires at the end of its useful life (or as a result of unfortunate events). **WorkLife™** ensures that our audiences of managers and employees at every level understand their accountability in the application of protective controls at every stage of the information's life. And it helps that we internally practice what we preach, from encrypting sensitive and back-up data, to ensuring that mobile information (and data in transit) are protected by adequate confidentiality controls, supplemented and enforced by the right administrative security practices.

6. *Visibility and Transparency* — Keep it Open

We believe that secrecy has its place in the world of information security, and leverage the concept internally to a significant degree. However, the concept is often misunderstood and when it comes to inadequate program management, security and privacy are both hindered by an overzealous application of "security by obscurity". This is why our **WorkLife™** Education, **Risk Advisor™**, **FlexProtect SPM™** and **FlexSecure Verify™** solutions all rely on protective controls that are in daily use internally to create a resilient 'shell' as well as a strong 'core' for Informatica as well as for any organization that wishes to adopt our practices. We believe in '**trust when verified**', in particular using our **Verify™** risk assessment methodology which we apply and perfect internally to ensure that it delivers both compliance (with PbD and visibility). In so doing, we ensure the clarity of an effective framework of protective controls as well as visibility into the risk posture of systems, applications and processes. **Transparency, when implemented correctly, is as much a mechanism for proper risk governance as it is an integral tool in ever privacy strategy**. And we demonstrate this by using examples from our own organization

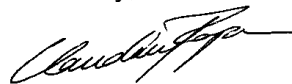
during **WorkLife Executive Briefings™**, **Security and Privacy Clinic™** and **Security & Privacy Awareness Certification™** programs for our employees and those of our valued clients.

7. *Respect* for User Privacy — Keep it *User-Centric*

Our internal project management practices are focused on information protection and place us at the core. From these we derived **FlexProtect SPM™** and **PPM™** project management services which focus on IT, security and privacy projects with discernible facets of risk. In so doing, we continue to improve our internal processes with external services, thus creating a cycle of continuous improvement and deeper application of Privacy by Design principles. In all cases, we manage projects and advise in the design and development of systems, applications and processes; from a responsible standpoint where the user is at the core of the process. Users are the reason for the design which needs to envelop, adapt and be flexible to their needs, while ensuring data protection. This is also at the core of our internal management of private data records, in particular in instances where we collect sensitive information about individuals. Our processes are designed to protect that information at all times, and our applications are configured to support and complement those processes. **Communication is a key part of this approach, as we insist on knowledge transfer to clients and keep users informed and aware.** This is a strategic approach we practice internally at Informatica, teach in our **WorkLife™** Education, enforce within our **SPM™** project management, consult on as part of our Risk Advisor™ (enterprise risk consulting) solution, and validate as part of our Verify™ security and privacy assessments.

We take pride in our role as a security and privacy leader. As such, we continue to adapt to changes in the industry and in the threat landscape while carefully listening to client needs so as to be able to meet *and* anticipate them. Our commitment to security and privacy includes a strategy for continuous improvement that includes on-going investment in education and controls that enable us to keep innovating and delivering solutions of the highest quality. Our internal processes are symbiotically connected to externally facing client solutions to improve our own practices, our company's adherence to PbD and in turn the process of improving the solutions we offer. We are proud that in so doing we are able to support and demonstrate the proper application of the **Privacy by Design Principles**, a valuable concept – and now a standard – pioneered by the Office of the Information and Privacy Commissioner of Ontario.

Sincerely,



Claudiu Popa, CISSP, PMP, CISA, CIPP
President, Informatica Corporation