

Personal.com

Privacy by Design Organizational Ambassador

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

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, PbD comes before-the-fact, not after.

Personal, Inc.'s mission is to give individuals ownership and control over their own personal data. Central to this mission is the privacy, security and trust of our users, who we call "data owners." Our system and product are fueled and guided by these considerations every step of the way. Indeed, we have developed and deployed strong privacy and security safeguards throughout our technological architecture and owner functionality, some of which are extraordinary for any company. The following are examples:

- All sensitive data must be locked and unlocked with an owner-chosen password that Personal does not store and, therefore, cannot access. Only the owner knows the password to unlock this information.
- If an owner forgets his or her password and needs to reset it, sensitive data will be deleted, and the individual will need to re-enter it. This is done for the owner's own protection and because Personal has no access to it as the previous point illustrates.
- Personal uses 256-bit SSL encryption to prevent others from eavesdropping on users. All pages and APIs involving the exchange of passwords or personal information are safeguarded in this way. We use secure cookies with HTTPS to further protect owner data.
- Any instance of sharing data within Personal is a "data-owner"-initiated event. When owners indicate they wish to share information, they are asked to confirm their intention. By the same token, Personal never imports owner data from other sites without the owner's explicit permission.
- We don't allow others to track owners while they are on Personal, and Personal does not track individuals when they leave the website.
- Personal has spent significant resources to avoid using third-party analytics and other tools that "phone home" and reveal what you do on Personal.

2. Privacy as the Default Setting

We can all be certain of one thing — the default rules! PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

As illustrated above, privacy is absolutely the default setting for Personal owners. Our products were designed with this principle in mind. Importantly, sharing data occurs only on a permission basis and within the context of sharing it. Data at rest is just that — data at rest.

3. Privacy Embedded into Design

PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

In addition to IT systems, PbD permeates Personal's business practices. For example, when individuals join Personal, owners sign an Owner Data Agreement -- <http://www.personal.com/how-we-protect-you/legal-protection> -- that turns the tables on the typical, long, unreadable legal agreements that sites or apps make users sign. This legally binding contract is the first of its kind, and it ensures owners own the data they choose to manage in Personal – not the company, others in the system or our corporate partners.

Among other things, the Owner Data Agreement states that:

- **The owner owns his or her data.** Under the terms of the agreement, the owner owns all the data managed in his or her Personal account.
- **The owner controls who gets access.** Only the owner can grant access to his or her data stored within Personal. Furthermore, Personal will never grant any third party access to owner data, except when specifically required by law. Even in those cases, the company will be unable to provide sensitive data, as only the owner has access to the password to decrypt it.
- **Our other owners and corporate partners will be legally obligated to recognize the owner's data ownership and will have to use owner data as prescribed in the agreement.** Any registered owner or partner with whom an owner chooses to grant access to his or her data will also have agreed to the same terms and conditions governing the use of the original owner's data.

- **Requirements data users must never violate.** Other owners in the system and partners may not access, use, store, share, or monetize owner data that is shared with them without explicit consent of the initial owner. Our partners must agree to be transparent about how they use owner data.
- **You *can* take it with you.** We have built a true delete button into the system, so that owners can permanently delete their information from Personal. In addition, owners can promptly export their own data at any time if they choose to leave Personal and would like a copy of their data.

4. Positive Sum

PbD seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

At Personal, privacy, security and functionality were built into our product from the outset. We have demonstrated that it is possible to create a people-centric platform that embeds all these principles into the company’s DNA, without trade-offs. The result is a secure personal data vault that empowers individuals to own, control access to and benefit from their information. Several of our strongest technical innovations are focused on securely storing data and sharing it within Personal.

5. Full Lifecycle Protection

PbD, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that, at the end of the process, all data are securely destroyed, in a timely fashion. Thus, PbD ensures cradle to grave, lifecycle management of information, end-to-end.

Personal was built with security embedded in its product from the beginning and is designed to last throughout the owner’s experience and lifecycle use of our product. Below are examples of some of our features, some of which bear repeating from Response 1:

- We use 256-bit SSL encryption from browser to storage, and https pages with secure cookies.
- As described in Response 4, the company offers innovative legal protections for owners at Personal.
- Data entered into fields marked “sensitive” can only be locked or unlocked with a password that only the data owner knows. If he or she forgets the password and

requires Personal to reset her password, all sensitive data is deleted. This is done to protect the data owner.

- Personal believes individuals should always be in control of their data, so we provide full portability and deletion powers. At any time, the data owner can export his or her data stored in Personal and delete all traces of the account. Currently, it takes 14 days to delete all of a person's data from the system, including logs, and we expect this lag to be shortened over time.

6. Visibility and Transparency

PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

We believe people should know who has their information, what is being collected about them, and how it is used. This means providing full transparency and choice about what data to manage on the site and how they wish to share or benefit from it. The Personal data owner alone is in control over what to save in the vault, whether to grant access to discrete information within it, and if so, to whom. Our website makes these points clearly. Regarding independent verification of our security procedures, we regularly conduct audits of our security architecture and have SSL certificates from VeriSign and GeoTrust. In addition, we are in the process of acquiring other third party seals and approvals such as TRUSTe privacy policy validation and others.

7. Respect for User Privacy

Above all, PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Personal was founded on the idea that the time had come for a true people-centric model for ownership and control of individual data online. At Personal, individuals have the rights to: data ownership; control; privacy; portability; and deletion. In turn, it is incumbent upon Personal to provide its owners with transparency, security and strong privacy safeguards.

Respect for individuals is at the core of our company. For example, as noted above, we call our users "data owners" instead of "users" or "consumers," as it is a constant reminder of who is in control of data at Personal. We empower people with their data and will help them to understand how to use it to take control over and improve their lives.