
# A Privacy Risk Framework for the Lead Generation Industry

by boberdoo.com LLC

## Introduction

Data collection, processing, and exchange is the heart of the Lead Generation Industry, also known as the Leads Industry (or Online Marketing Industry). It is used to develop, market, and sell products and services that consumers want or need, creating value for our businesses and consumers (individuals) alike. Operating in this space comes with many inherent risks for businesses and individuals that must be thoughtfully managed, not only to maintain compliance with regulations, but because it is the right thing to do. As a commitment to privacy, we advocate and practice the following principles:

- ★ We believe that data is a valuable asset and should be protected accordingly to ensure the confidentiality, integrity, and availability of the data under our care.
- ★ We embrace best practices, industry standards, and evolving regulations because we believe they make us, and our industry, better.
- ★ We adapt our business to meet and exceed the security and privacy expectations of our clients and partners.
- ★ We promote security awareness and transparency among our employees, consumers, and industry partners.
- ★ We pursue continuous improvement in security and privacy practices to protect our employees, clients, and consumers against evolving threats.
- ★ We encourage and enable clients to implement robust data retention and deletion policies because we believe that lead companies should retain data only as long as required to provide the requested service to consenting consumers - **not forever**.

Privacy is a priority for us as it is, and should be for all of us in the Lead Generation Industry ecosystem. We present the following Privacy Risk Framework for your consideration and use in developing a privacy risk management program for your business. Whether you are just beginning your privacy journey or assessing your current privacy program, this framework is a good place to start or enhance your privacy protection initiatives. The framework components within this document include:

- A definition of data privacy
- The reasons for adopting a privacy risk framework
- Makes a distinction between security and privacy
- Includes a set of checklists based on the NIST Privacy Framework
- Presents a variety of methods for treating privacy risk
- Maps boberdoo Lead Management System features to core functions of the privacy framework
- Concludes with a list of references and resources for continued exploration

The framework is intended to support the development of your privacy program and should be customized to align with your organization's unique values and specific needs in response to compliance requirements and your data protection commitments.

# What is data privacy?

Data privacy is the relationship between the collection and processing of data, the public expectation of privacy, and the legal and regulatory issues surrounding them. It is also known as information privacy or data protection but will be referred to as data privacy throughout this document.

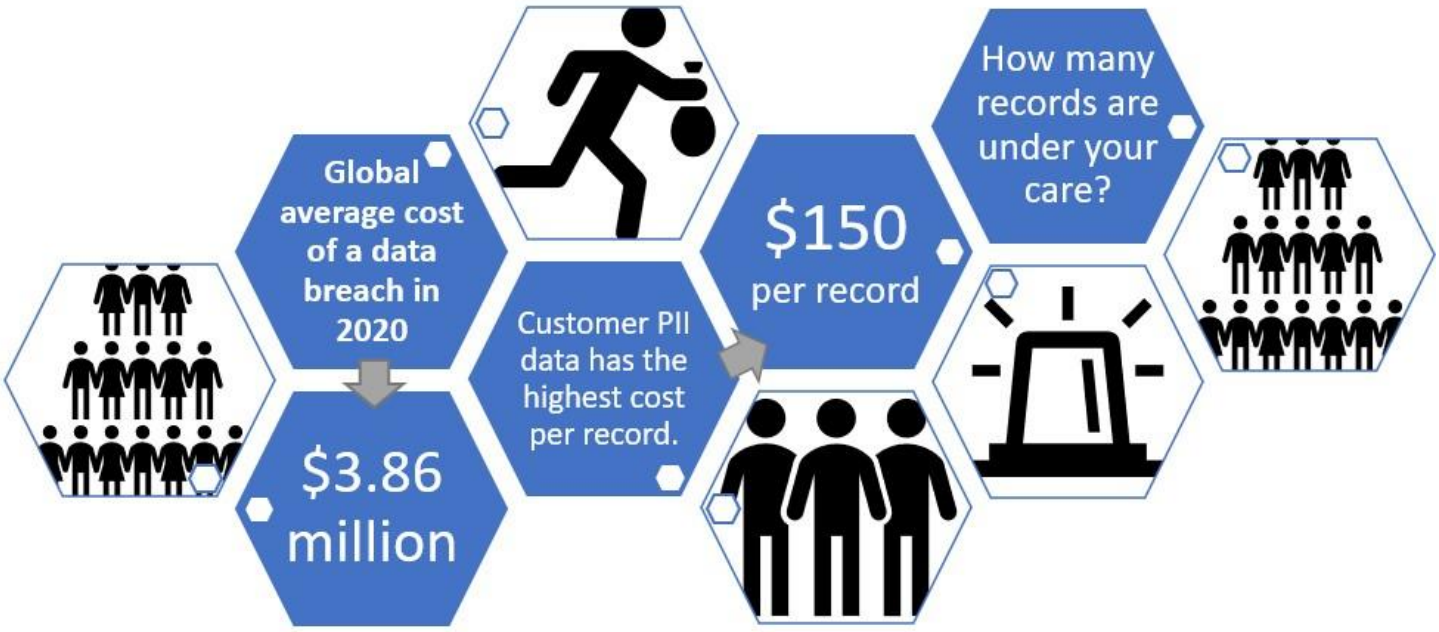
Data Privacy or Information privacy encompasses:

- A focus on the rights of individuals giving them control over their personal data
- Procedures for proper handling, processing, collecting, and sharing of personal data
- Compliance with data privacy laws such as CCPA or GDPR

# Why use a privacy risk framework?

The risks associated with ignoring or inadequately tending to privacy are great. Untreated privacy risk can quickly lead to a data breach and non-compliance with regulations resulting in hefty fines and huge costs that can be avoided with proper data privacy policies, procedures, and practices.

A Privacy Framework can assist an organization to optimize its data processes and develop products and services that respect the privacy of individuals and maintain compliance with data privacy laws.




IBM Cost of a Data Breach Report 2020

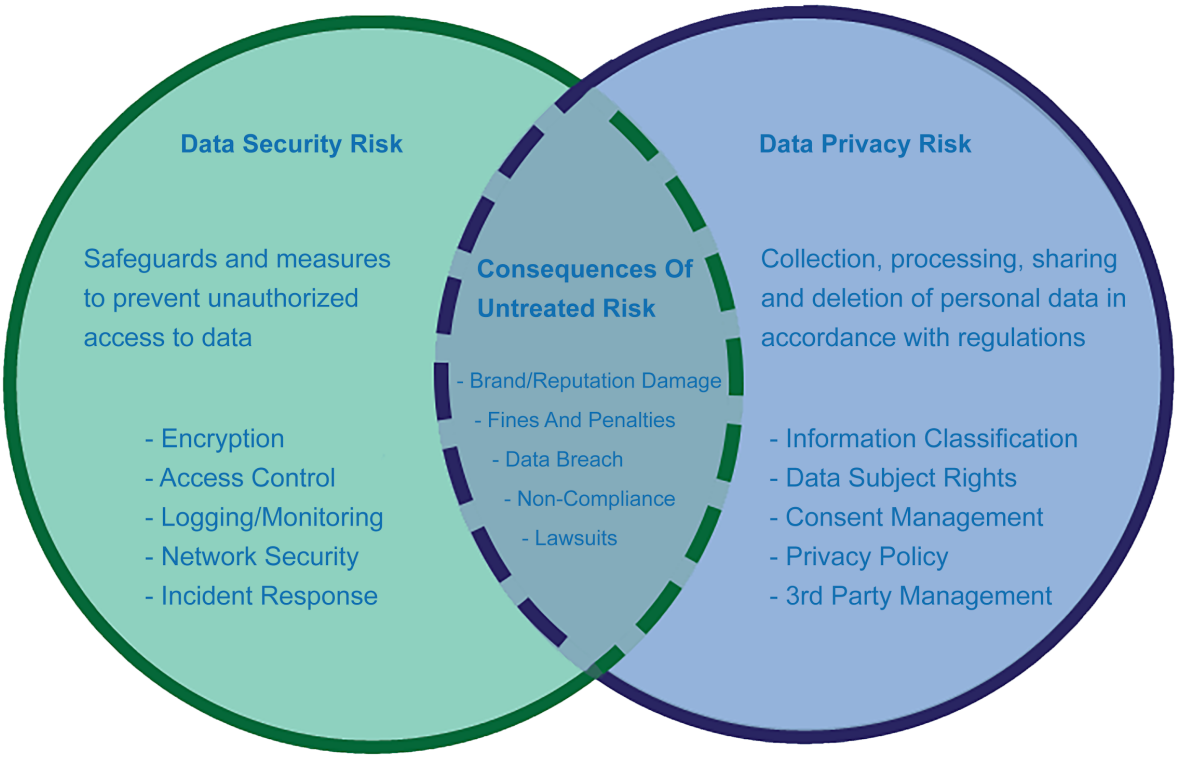
# Security vs. Privacy

To properly protect data and comply with data protection laws, you need both Data Privacy and Data Security. This makes sense because security and privacy are complementary. Data privacy addresses many concerns such as:

- ➔ **Collecting only the information you actually need and disposing of it when no longer needed**
- ➔ **Being transparent about your use of personal data and how it is processed, shared, and stored**
- ➔ **Maintaining the privacy rights of individuals according to data protection regulations**

Data Security, on the other hand, includes measures that an organization can take to prevent any third party from unauthorized access to personal data. It focuses on the protection of data to prevent privacy-related risks from becoming incidents such as misuse of information, disclosure of personal information, denial of a data subject's rights, or violation of privacy laws. It includes security measures such as access control, encryption, and network security.

Data security is partially addressed in the privacy framework, however, it is expected that businesses maintain a comprehensive security program and adopt a cybersecurity framework that addresses enterprise risk beyond privacy matters alone.




# About the Privacy Framework

A Privacy Framework is a voluntary tool that can help your organization create or improve a privacy program as well as aid in compliance with different data protection regulations around the world. Effective privacy risk management can help you build trust in your products and services, communicate your privacy practices, and meet your compliance obligations. This data privacy framework provides a structured approach to data privacy management and is designed to support privacy-by-design concepts.

The Privacy Framework has its foundation in the NIST Privacy Framework; a subset of functions and categories from the NIST framework is presented here and tailored to the interests of the Lead Generation Industry. The intent is to aid organizations in creating or enhancing an existing framework for their business and guide an organization towards the implementation of controls best suited to addressing their privacy risk profile. A control is an action or measure that can be undertaken to reduce privacy risk. Controls may include policies, processes, procedures, or technical measures that satisfy the guidance of the framework categories. The adoption of a privacy framework should culminate in an action plan for privacy management improvements and should be regularly updated and evaluated to measure the progress of your privacy program.

# A privacy framework for YOUR business

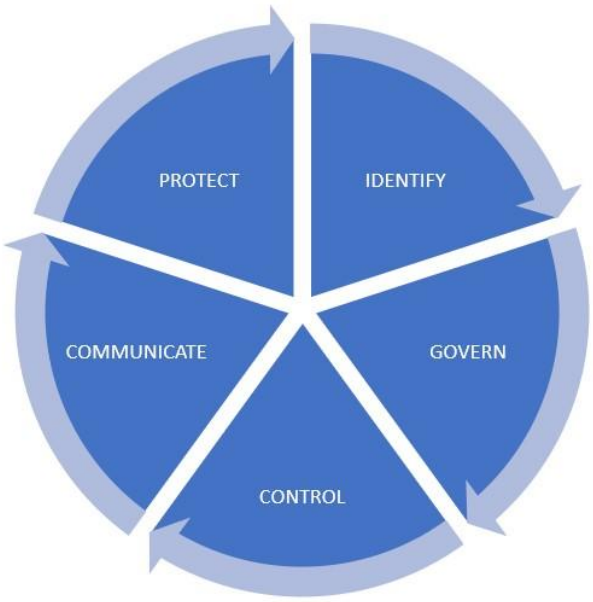
Every business is unique. Depending on your role in the Lead Generation Industry and your organization's risk appetite, the framework should be customized to address your priorities for managing privacy risk. When adopting a framework, select the risk categories and implement controls based on the needs of your organization considering factors that align with your risk management strategy.

- ➔ regulatory requirements and industry standards (CCPA, GDPR, HIPAA, PCI, etc.)
- ➔ your products, services, systems, and related data processing activities
- ➔ shared privacy responsibilities with third parties (ecosystem)

Implementation of a privacy framework should begin by assessing the strength of privacy measures your company currently practices and then develop a plan for improvement in your company's capability to manage privacy risk.


*The Lead Generation Ecosystem*

# Privacy Risk Management Functions




The framework is organized into five functional areas and then subdivided into numerous categories and subcategories. The five functions are: **Identify, Govern, Control, Communicate and Protect**. The categories and subcategories drill deeper into areas of concern leading you to the real actions that can be taken to manage privacy risk. Select subcategories are presented below. These are intended for organizations that may be beginning their privacy journey or those that wish to establish a baseline for their new or existing privacy program.

The following tables may be used as a set of checklists to assess your current posture and identify areas of the business that need attention. The **QUICKSTART** column presents "quick wins" or actions that can be undertaken quickly before moving on to more advanced capabilities depending on the needs of your organization.

## Identify Privacy Risks

Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

| [IDENTIFY] NIST Privacy Framework Categories | QUICKSTART |
|---|---|
| ❑ **Inventory and Mapping**<br>❑ Systems/products/services that process data are inventoried.<br>❑ Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.<br>❑ Data actions of the systems/products/services are<br>❑ Inventoried.<br>❑ The purposes for the data actions are inventoried.<br>❑ Data elements within the data actions are inventoried.<br>❑ The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).<br>❑ Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services. | Identify the data you are processing (such as collecting, using, sharing, storing) and map out its flow through your systems throughout the full data lifecycle – from collection to disposal. |
| ❑ **Business Environment**<br>❑ The organization's role(s) in the data processing ecosystem are identified and communicated. | Understand your role in the industry ecosystem and how it relates to 3rd parties and individuals. |

| | |
|---|---|
| ❑ Priorities for organizational mission, objectives, and activities are established and communicated. | |
| ❑ **Risk Assessment**<br>❑ Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.<br>❑ Risk responses are identified, prioritized, and implemented. | Conduct a privacy risk assessment to assess your data processing activities and their impact on individuals. |
| ❑ **Data Processing Ecosystem Risk Management**<br>❑ Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.<br>❑ Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program. | Evaluate contracts and select products and services you use to run your business that align with your privacy priorities. |

# Govern Privacy Risks

Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

| [GOVERN] NIST Privacy Framework Categories | QUICKSTART |
|---|---|
| ❑ **Governance Policies, Processes, and Procedures**<br>❑ Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.<br>❑ Roles and responsibilities for the workforce are established with respect to privacy.<br>❑ Legal, regulatory, and contractual requirements regarding privacy are understood and managed.<br>❑ Governance and risk management policies, processes, and procedures address privacy risks. | Know your privacy-related legal obligations so that you can build compliant products and services. |
| ❑ **Risk Management Strategy**<br>❑ Risk management processes are established, managed, and agreed to by organizational stakeholders. | Conduct regular risk assessments and plan actions to reduce privacy risk. |
| ❑ **Awareness and Training**<br>❑ The workforce is informed and trained on its roles and responsibilities. | Provide your employees with privacy awareness training. |

| | |
|---|---|
| ❑ Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities. | |
| ❑ **Monitoring and Review**<br>❑ Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., the introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.<br>❑ Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.<br>❑ Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place. | Regularly reassess to see if your privacy risks have changed. |

# Control Privacy Risks

Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

| [CONTROL] NIST Privacy Framework Categories | QUICKSTART |
|---|---|
| ❑ **Data Processing Policies, Processes, and Procedures**<br>❑ Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).<br>❑ Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.<br>❑ A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems. | Are you collecting, sharing, or keeping data that you don't need? Consider how your policies help you or other organizations maintain control over data |
| ❑ **Data Processing Management**<br>❑ Data elements can be accessed for review.<br>❑ Data elements can be accessed for deletion.<br>❑ Technical measures implemented to manage data processing are tested and assessed. | Take your privacy risks and legal obligations into account when deciding on the functionality of your systems, products, or services. |
| ❑ **Disassociated Processing**<br>❑ Data is processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization). | Implement technical measures such as de-identification, |

| | |
|---|---|
| ❑ Data is processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization). | decentralized data processing to protect consumer's identity |

# Communicate Privacy Risks

Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data is processed and associated privacy risks. Both organizations and individuals may need to know how data is processed in order to manage privacy risk effectively.

| [COMMUNICATE] NIST Privacy Framework Categories | QUICKSTART |
|---|---|
| ❑ **Communication Policies, Processes, and Procedures**<br>❑ Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.<br>❑ Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established. | Craft policies for communicating internally and externally about your data processing activities. |
| ❑ **Data Processing Awareness**<br>❑ Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.<br>❑ Impacted individuals and organizations are notified about a privacy breach or event.<br>❑ Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions. | Consider what you will do in case of a data breach. E.g. How will you provide notifications or any remedies such as credit monitoring or freezes? |

# Protect Against Privacy Risks

Develop and implement appropriate data processing safeguards.

| [PROTECT] NIST Privacy Framework Categories | QUICKSTART |
|---|---|
| ❑ **Data Protection Policies, Processes, and Procedures**<br>❑ A baseline configuration of information technology is created and maintained incorporating security principles (e.g., the concept of least functionality). | Implement formal change management processes, incident response policies, and recovery |

| | |
|---|---|
| ❑ Configuration change control processes are established and in place.<br>❑ Backups of information are conducted, maintained, and tested.<br>❑ Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.<br>❑ A vulnerability management plan is developed and implemented. | plans. |
| ❑ **Identity Management, Authentication, and Access Control**<br>❑ Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.<br>❑ Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.<br>❑ Network integrity is protected (e.g., network segregation, network segmentation). | Develop access management policies according to the principle of least privilege. |
| ❑ **Data Security**<br>❑ Data-at-rest is protected.<br>❑ Data-in-transit is protected.<br>❑ The development and testing environment(s) are separate from the production environment. | Encrypt sensitive data, at rest and in transit. |
| ❑ **Maintenance**<br>❑ Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. | Update security software regularly, automating those<br>updates if possible. |
| ❑ **Protective Technology**<br>❑ The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.<br>❑ Communications and control networks are protected. | Maintain and analyze system/user activity logs.<br><br>Implement firewalls, ACLs, IDS to detect and prevent unauthorized network access. |

# Strategies for Managing Privacy Risk

After you have used the framework to assess your current state and identify areas for improvement, you will need to decide how to make improvements aimed at reducing your risk. There are four main ways to treat privacy risk. Each method should be evaluated to determine what approach will be most effective and cost-efficient for your business.

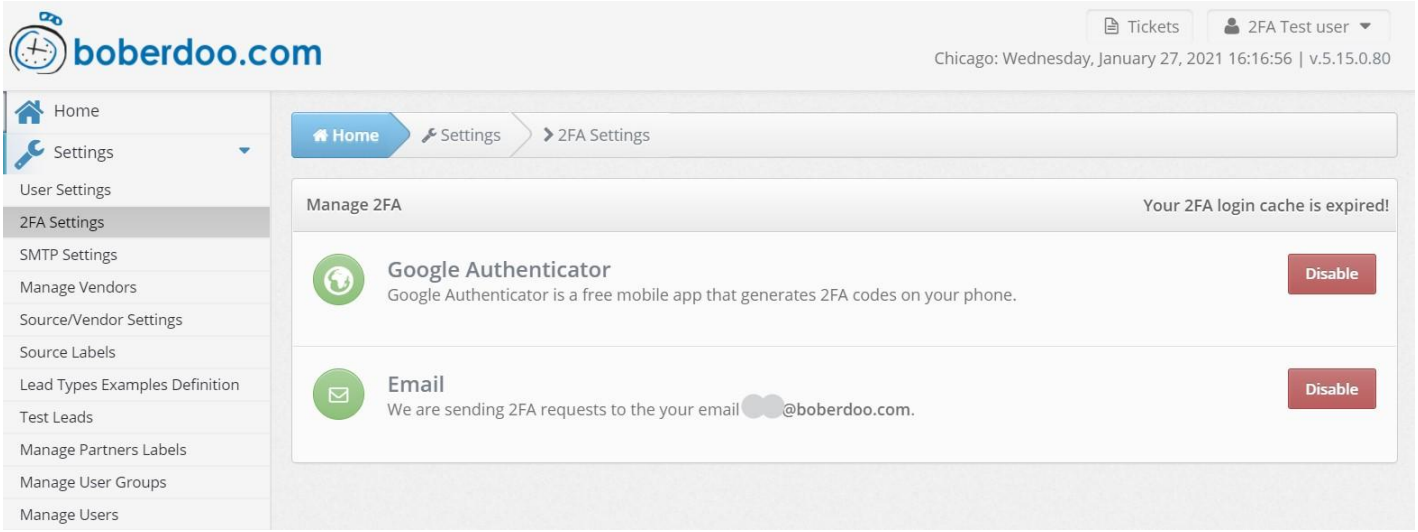
- **Mitigate the risk:** Integrating data privacy measures into your IT systems, organizational processes, and products and services.
- **Transfer the risk:** Delegating the responsibility to third parties, such as a cloud service provider, or using a consent mechanism to share responsibility with data subjects. The most common form of risk transfer is CYBER INSURANCE.
- **Avoid the risk:** Ceasing data collection where the risks outweigh the benefits. If you don't need it, don't store it.
- **Accept the risk:** Concluding that remedial action is unnecessary because the potential damage is either minimal or highly improbable.

The decision on how to treat risk is up to you and is often a combination of the methods listed above. Factors to consider when deciding how to address risk areas include your position in the industry ecosystem, your business model, your current capabilities, and your risk appetite.

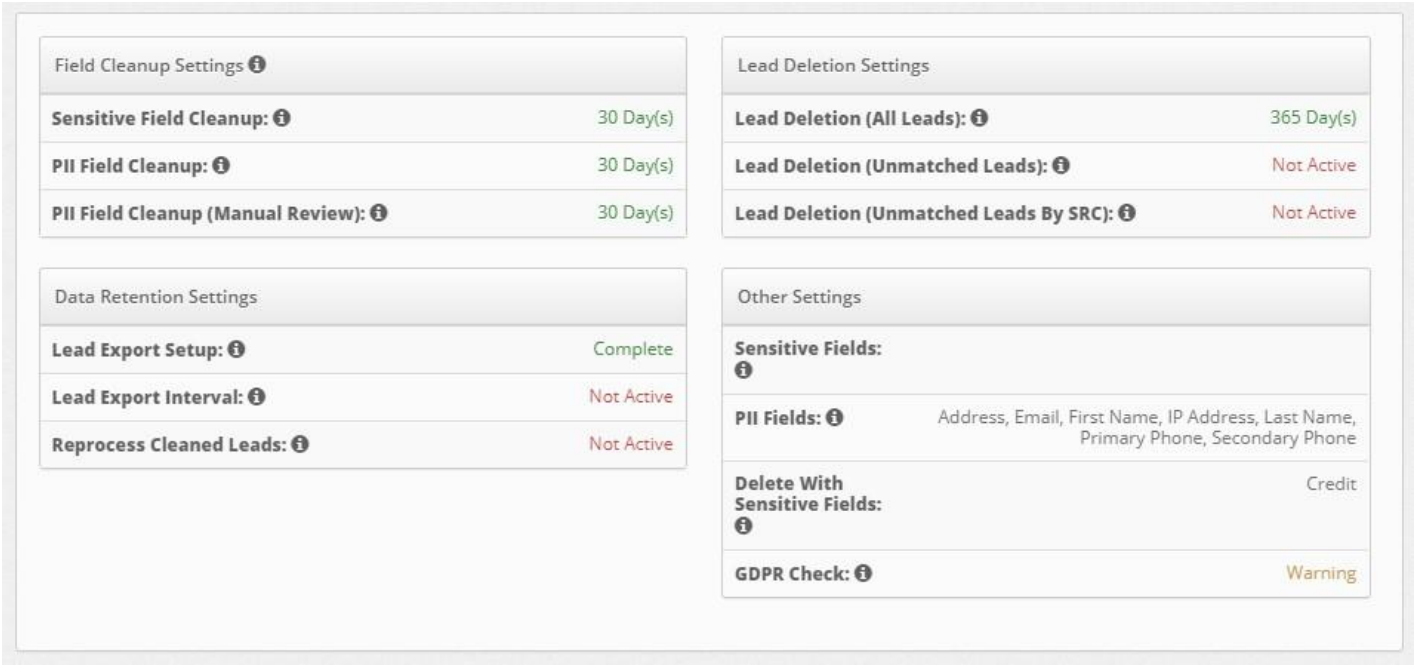
## How a boberdoo Lead Management System can help you manage privacy risk

boberdoo Lead Management Systems are purpose-built to include features and capabilities with privacy in mind. In other words, we practice **privacy by design**. When assessing, designing, and implementing your products, services, and systems, as well as those of your partners, it is important to consider privacy risk from the very beginning. Look for features and capabilities that directly align with your privacy framework and your organization's values. The following table presents select boberdoo LMS features and maps them to one or more of the privacy framework's core functions. You can do the same feature mapping for your own products or services and for 3rd party systems and services that are part of your particular business processes.

| Select Lead Management System Features | Privacy Framework Function |
|---|---|
| **Login Security**<br>Two-factor authentication set at the user-level for logins to the boberdoo system. | **PROTECT** |

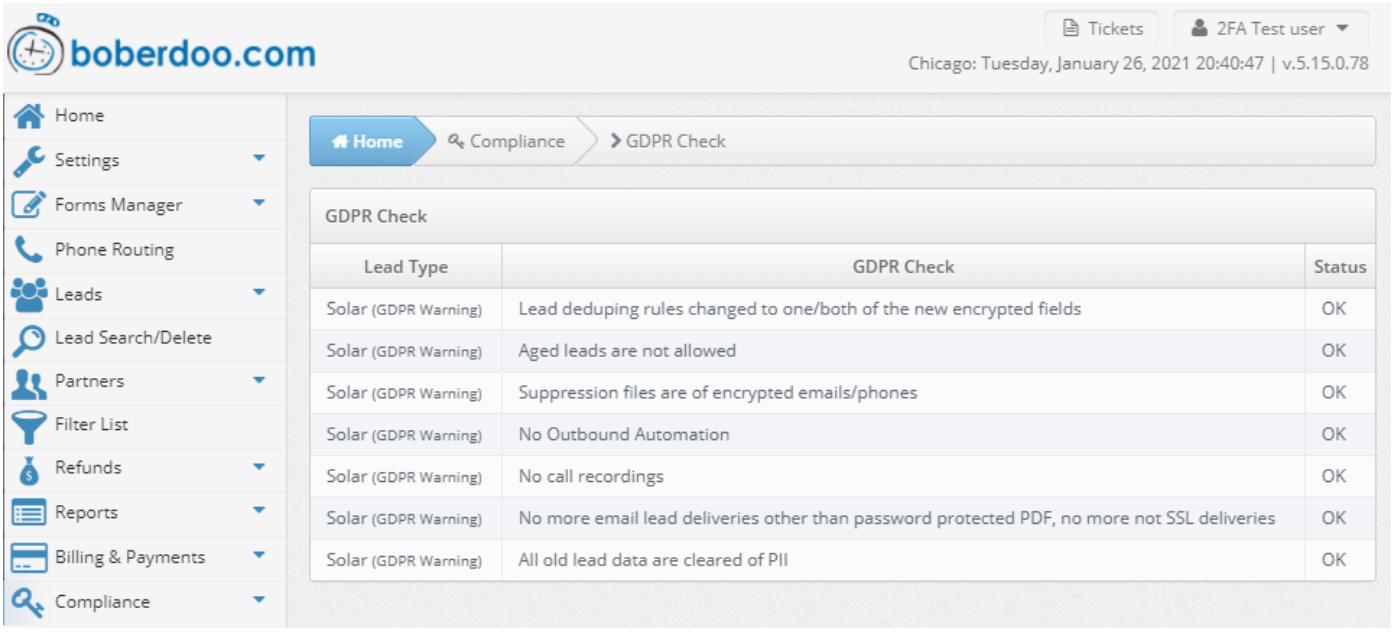



| | |
|---|---|
| **Lead Field Security**<br>Sensitive data encryption with access via Secure Mode. | **PROTECT** |
| **Compliance Tab**<br>Stay compliant with data laws and keep track of security features all from one tab. | **IDENTIFY**<br>**COMMUNICATE** |
| **Secure Data Retention**<br>Automated and bulk secure export to store encrypted data in your Amazon Web Services account. | **PROTECT** |




| | |
|---|---|
| **API Keys**<br>Secure your API functions by using API key restrictions. | **PROTECT** |

| | |
|---|---|
| **Sensitive Field Encryption**<br>When building your lead types, any fields universally known as sensitive, such as Social Security Number and account numbers, are automatically encrypted in the database and front-end once posted into the boberdoo system. | **PROTECT** |
| **Secure Mode**<br>In order to decrypt and view sensitive field values or access any features that display sensitive data, users must activate Secure Mode. Secure Mode requires password verification and logs all activity related to sensitive fields. | **PROTECT** |
| **30 Day Sensitive & PII Field Cleanup**<br>All sensitive fields are set to automatically delete from your boberdoo system after 7 days. Personally Identifiable Information (PII) fields are set to automatically delete from your boberdoo system after 30 days. We can shorten this deletion timer or securely export fields to your Amazon S3 account before deletion | **CONTROL** |
| **365 Day Lead Deletion**<br>The entire lead data is deleted after 365 days in the system. This deletes even the hashed values used for duplicate checks. We can shorten this deletion timer or securely export leads to your Amazon S3 account before deletion. | **CONTROL** |




| | |
|---|---|
| **Existing PII & Sensitive Field Cleanup**<br>All existing PII and sensitive data is cleared from your system. The lead ID and remaining data is still stored in your system, but the PII and sensitive fields are deleted. | **CONTROL** |

| | |
|---|---|
| **Real-Time Email & Phone Hashing**<br>All email and phone fields are hashed before being cleaned in real-time. This allows you to search for leads via email and phone and continue using email and phone as dedupe fields. | **CONTROL** |
| **Secure Lead Deliveries Only**<br>No standard email or non-SSL lead deliveries are allowed. If currently in-use, these deliveries will fail upon attempt. Only PDF emails with passwords and secure custom deliveries are allowed. | **CONTROL** |
| **Whole Lead Deletion After 365 Days**<br>All remaining lead data is deleted from your system after 365 days. This includes hashed email and phone fields which, after deletion, can no longer be searched or used for deduping. | **CONTROL** |
| **Historic Bulk Data Export**<br>Bulk export all existing data in your system. This can be done before the mandatory PII and sensitive field cleanup or after the cleanup is complete. | **PROTECT** |
| **Contact Search And Cleaning Tool**<br>Search for contacts via email or phone to provide customers their information, update fields or clean data upon request. | **GOVERN** |

# References and Resources

**The Shared Responsibility Of Information Security (boberdoo blog)**
https://www.boberdoo.com/news/the-shared-responsibility-of-information-security-and-privacy

**How Risk Management Can Prevent A Data Breach Webinar - YouTube** (a boberdoo U webinar)

**NIST Privacy Framework:** https://www.nist.gov/privacy-framework

**AICPA Privacy Management Framework:**
https://us.aicpa.org/interestareas/informationtechnology/privacy-management-framework

**ISO/IEC 27701 – International Standard for Privacy Information Management**
https://www.iso.org/

**Stay Safe Online — NCSA:** https://staysafeonline.org/data-privacy-day/

**International Association of Privacy Professionals — IAPP:** https://iapp.org/

**US State Comprehensive Privacy Law Comparison:**
https://iapp.org/resources/article/state-comparison-table/

**Cost of a Data Breach Report 2021:** https://www.ibm.com/security/data-breach

**Are You Doing Enough to Protect Your Customers' Data?** - NCSA:
https://staysafeonline.org/resource/protecting-customer-data/

---

**boberdoo.com is #PrivacyAware.** We recognize and support the principle that all organizations share the responsibility of being conscientious stewards of personal information. We support the NCSA and our partners in promoting privacy awareness on Data Privacy Day and throughout the year.


**The National Cyber Security Alliance has offered up the following tips to help guide individuals and businesses to better data privacy practices, such as:**

- **If you collect it, protect it.** Data breaches can not only lead to great financial loss, but a loss in reputation and customer trust. Follow reasonable security measures to keep individuals' personal information safe from inappropriate and unauthorized access. Make sure the personal data you collect is processed in a fair manner and only collected for relevant and legitimate purposes.
- **Consider adopting a privacy framework.** Build privacy into your business by researching and adopting a privacy framework to help you manage risk and create a culture of privacy in your organization.
- **Conduct an assessment of your data collection practices.** Understand which privacy laws and regulations apply to your business. Educate your employees of their and your organization's obligations to protecting personal information.
- **Transparency builds trust.** Be open and honest about how you collect, use and share consumers' personal information. Think about how the consumer may expect their data to be used and design settings to protect their information by default. Communicate clearly and concisely to the public what privacy means to your organization and the steps you take to achieve and maintain privacy.
- **Maintain oversight of partners and vendors.** If someone provides services on your behalf, you are also responsible for how they collect and use your consumers' personal information.

## About boberdoo.com LLC

boberdoo.com is a SaaS solution for the lead generation industry. Whether you're new to lead generation and looking to automate your business or a lead gen veteran looking to maximize your revenue-per-lead, boberdoo is here to help. We've been helping lead companies grow their businesses since 2001 and we'd be happy to help you too. There are enough things to worry about in the lead industry. Your lead distribution software shouldn't be one of them.

Author: Dan Cerceo, CISSP, Chief Information Security Officer, boberdoo.com LLC
Contributors: Brad Seiler, Owner, boberdoo.com LLC; Scott Hettman, Head of Sales; Taylor Leikness, Graphic Designer