CSR Readiness® Pro Edition

Frequently Asked Questions

June 2015

Confidential and Proprietary

CSR Readiness FAQs Training

CSR Readiness® Pro Edition
Frequently Asked Questions

Securing Personal Data and Preparing for a Breach are Critical

What is CSR Readiness® Pro Edition?

The CSR Readiness® Pro Edition comprises the risk assessment program CSR Readiness® and the *award-winning* CSR Breach Reporting Service™ (BRS).

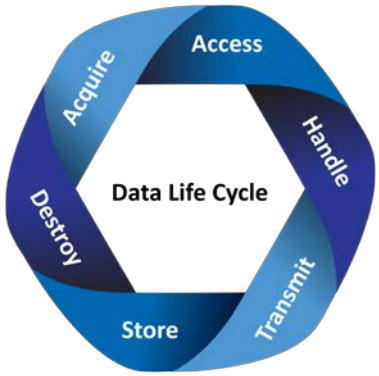
How does the CSR Readiness® Program work?

CSR Readiness® Program is an online self-assessment tool that helps you review, revise and revisit your business processes for handling the personally identifiable information (PII) of your customers, employees and vendors as required by a host of legislation and regulations.

CSR Readiness® 3 Step Process:

1) Review – Take a Self-Assessment Evaluation

- Detect location of personally identifiable information (PII) in an organization
- Determine how PII is:
  - ✓ Acquired
  - ✓ Accessed
  - ✓ Handled
  - ✓ Transmitted
  - ✓ Stored
  - ✓ Destroyed



2) Revise – Implement Readiness Policies and Remediation Instructions

- Remediate weaknesses and train employees on system-generated policies and procedures

3) Revisit – Continually Improve Risk Score

- Routinely monitor and audit performance to meet legal, regulatory and other compliance requirements

A dashboard will show progress and generate tasks to improve compliance. You can improve your business risk scores by remediation and implementation of further program offerings. Upon successful completion of the analysis and remediation, your business will earn a Certificate of Completion and the ID Stay Safe Digital Seal that you can use on your website and advertising.

What does the Certificate of Completion signify?

Once a business has completed all the questions in the self-assessment evaluation and implemented the remediation tasks, you will be awarded the Certificate of Completion. This can be placed on your website and is valid for one year from date of issue. By annually revisiting your self-assessment, you can maintain this Certificate of Completion.

What does CSR Breach Reporting Service do for me?

In the event of the actual or suspected breach of PII, the CSR Breach Reporting Service reports to authorities and notifies consumers, as required.

Your call to the in-house CSR team of privacy professionals initiates a custom evaluation of your incident to determine if authorities and consumers must be notified. CSR files the necessary breach reports on your behalf, and consumer notification can be prepared with your input.

Why do businesses need Readiness Pro Edition?

Various state, federal and international laws require businesses to protect the personally identifiable information of employees, vendors and customers. Penalties for noncompliance can include fines, prosecution and even jail time. Massachusetts and Connecticut are just two examples of many jurisdictions that require businesses that deal with their residents maintain comprehensive risk assessment, remediation and monitoring programs related to their handling of legally protected personal information, known as PII.

If organizations don't have this service, what could happen?

While it's impossible to completely avoid a breach due to uncontrollable circumstances, 97% could have been prevented. Accidents, errors and theft are just a few ways that information is compromised. Smart devices and wireless services compound the problem. Proactive detection and correction can go a long way to prevent loss and further fallout due to reputational damage, lost sales, fines, lawsuits and prosecution.

The Department of Homeland Security, the FTC, Visa and the BBB encourage businesses to protect consumer data and plan ahead to reduce risk. All states have laws that protect their residents who might be your customers, employees or vendors. Many laws specifically require creation and maintenance of information security programs by businesses that employ or have customers who are residents of those states. These laws include penalties for noncompliance.

For example, the civil penalty for violating the Connecticut Act No. 08-167, requiring safeguarding of personal data, is $500 per violation, up to $500,000 for a single event.

Lost trust means lost sales. The fallout of data breaches has caused businesses to close their doors. According to Visa, businesses should "Consider a breach likely and plan accordingly."

Definitions

What is personally identifiable information or PII?

The simple answer is it's anything that can be used to identify you. The loss of this information leads to identity theft.

Types of personal information include: name, address, phone, email, birthdates, Social Security numbers, driver's license, bank account and credit card information and the list continues to grow with new and revised legislation and court rulings.

Other personal information includes health information, medical records, Vehicle Identification Numbers, license plate numbers, login credentials and passwords, school records as well as voice recognition files. Fingerprints, retina scans, and handprints are also considered personal information.

What is the difference between PCI and PII?

PCI data is just one type of personally identifiable information. The PCI Data Security Standard protects credit cardholder data such as debit or credit card number, expiration date and card security code.

What is a breach of personally identifiable information?

The unauthorized access, loss, use or disclosure of information by either accident or criminal intent which can identify an individual.

What is data breach reporting?

When a breach occurs, the clock starts ticking to comply with federal, state and other laws. Reporting involves the where, when and how of the incident.

What is consumer notification?

Almost every state has enacted a data breach notification statute. These laws generally require businesses that have personal information about residents within a state to notify those residents when that data is compromised.

What are some examples of a breach?

A breach can occur in many ways, including through lost laptops or smart phones, improper disposal of paper records, or intrusion into your network or PC by hackers. The definition continues to expand.

What is ID Stay Safe?

Upon successful completion of the Readiness Program, users will earn a *Certificate of Completion* along with an ID Stay Safe digital seal to display on their company website. The seal remains valid for one year, at which time they will *Revisit* to ensure their business has sufficiently addressed any all changes that may have occurred throughout the year.

Requirements to Protect Data

What laws govern personally identifiable information?

Here are a few examples of the hundreds of laws and regulations that relate to the protection of personally identifiable information (PII) and requirements to report suspected or real loss:

- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Drivers Privacy Protection Act (DPPA)

- Drivers Privacy Protection Act (DPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic Clinical Health (HITECH) Act
- Payment Card Industry Data Security Standard (PCI-DSS)
- Family Educational Rights and Privacy Act (FERPA)
- 47 state data breach laws

Who are the enforcement agencies and others who might be involved after a breach?
Enforcement officials include various federal and state agencies as well as attorneys general, commissioners and others. Here are a few examples:

- Federal Trade Commission (FTC)
- Consumer Financial Protection Bureau (CFPB)
- Card brands like Visa, MasterCard, etc.
- State Attorneys General
- Federal Bureau of Investigation (FBI)
- US Secret Service
- Dept. of Health and Human Services/Office of Civil Rights

What if personally Identifiable information shared and/or received from another organization is compromised?
If your business is a third-party provider and has personally identifiable information on customers, employees, or vendors, then you may be required to notify authorities and/or consumers and others that a breach, or suspected breach, has occurred.

What if personally Identifiable information under my care is encrypted, redacted, or masked?
Even if the material is encrypted, redacted or masked, various regulations still require you to report. If it is encrypted, and the encryption key has been potentially compromised, reporting is required and/or notification is required.

How can I limit the threat of a data breach?
Almost everyone can do more to protect personally identifiable information. CSR Readiness® helps you assess your risk in handling PII, remediate your processes, implement policies, train staff and continue to monitor and audit, as required by laws and regulations.

Justifications

Why can't I do it myself?
You can try. However, liability rests entirely with you, as well as civil and criminal sanctions, on both state and federal levels. Trained, certified privacy professionals have developed a proprietary system to help you evaluate your circumstances against hundreds of rules and regulations to determine what remediation must be done, what policies implemented and provide you with the tools to train your employees as required by law.

What if I don't have any personally identifiable information?
Many organizations do not realize the personally identifiable information that they hold. If you have customers, employees or vendors, you have personal information that needs to be protected.

We don't deal with customers directly. I don't think my business needs this service.
If your business has personally identifiable information on customers, employees, or vendors, then you are required to safeguard that personal information.

I'll never get breached or hacked
Employees alone cause 75% of data breaches, whether intended or unintended. It's very likely that, at some point, data in your care, belonging to employees, customers or vendors will be lost, stolen or compromised. You are legally responsible and liable to implement and maintain a security program to safeguard PII data.

Technical

CSR's support team will handle all technical questions. These FAQs are included in the event you choose to provide theses answers when your customers call.

How do I begin?
To begin, simply go to <<Readiness URL>> to register and create credentials to begin the process. You will have 24/7 access to your account.

I forgot my username.
Your 'username' is the email address you registered with when signing up for Readiness. If you change your original registration email address using My Account in Readiness, this updated email address is your 'username'.

I forgot my password.
To retrieve your password, you will need the email address you entered during registration or the updated email address you associated with your account using My Account in Readiness. Click on the Forgot Password link on the Log In screen. Enter in your email address and click the Email Link button. A reset password link will be sent to that email address. Click on that link to reset your password. If you do not receive that email or have any problems resetting your password, please contact support@csrps.com for further assistance.

I skipped some questions and want to go back to them, how do I do that?
To navigate back to questions previously skipped you can use the Next and/or Back buttons located at the bottom of your questionnaire. You can also click on the Show Progress tab and click directly onto the domain of the question you would like to go back to. Before submitting your questionnaire you will also be prompted to complete any required questions that have not been answered, which you can choose to still not answer and submit your questionnaire.

I don't know an answer to a question – can I just skip it?
You can skip questions and come back to them later. You must answer all questions to proceed to the remediation phase of Readiness.

How long will it take to complete this assessment?
It is estimated that it will take one hour to complete the assessment. An assessment may take longer should consultation or research be required to answer to some of the questions. Progress within the assessment is saved as questions are answered. Therefore, you can leave the assessment and come back to it at a later time to finish. Your answers up to that point will be saved.

What is the ID Stay Safe seal?
This digital seal is a stamp that you can place on your website, which alerts your customers, affiliates, potential clients, corporate insurers, etc., that your organization has performed a thorough self-assessment on how your organization protects personally identifiable information, ensures you have policies in place to maintain a high level of vigilance, audit, and association education with regards to the protection of PII data within your organization.

How do I put the completion seal on my website?
Once the self-assessment has been taken and the recommended remediation tasks have been completed, an email will be sent to the associated account's registered email address with the certification seal as well as instructions on how to use it in materials and embed it on your web page. If there are any issues regarding the implementation of the completion seal, please contact **support@csrps.com** for further assistance.