Erste Schritte mit dem NIST Privacy Framework:
Eine Kurzanleitung für kleine und mittlere Unternehmen

„Es ist schwierig, für den Aufbau eines Datenschutzprogramms zu plädieren ... Das NIST Privacy Framework war eines der Werkzeuge, die wir nutzen konnten, auch wenn wir nicht in der Lage waren, ein großes Datenschutzteam zu besetzen."
- *Jaime Lees, Chief Data Officer, Regierung von Arlington County*

Was ist das NIST Privacy Framework und wie kann meine Organisation es nutzen?

Das NIST Privacy Framework ist ein freiwilliges Tool, das Ihrer Organisation helfen kann, ein Datenschutzprogramm zu erstellen oder zu verbessern. Ein effektives Datenschutzrisikomanagement kann Ihnen dabei helfen, Vertrauen in Ihre Produkte und Dienstleistungen aufzubauen, besser über Ihre Datenschutzpraktiken zu kommunizieren und Ihre Compliance-Verpflichtungen zu erfüllen. Eine gute Cybersicherheit ist wichtig, kann aber nicht alle Datenschutzrisiken beseitigen.

Beginnen Sie mit der Verwendung des Datenschutz-Frameworks, indem Sie einem einfachen Modell von „Ready, Set, Go"-Phasen folgen und Ihr Unternehmen oder Ihre Behörde auf fünf Bereiche des Datenschutzrisikomanagements ausrichten: identifizieren, steuern, kontrollieren, kommunizieren und schützen.

AUF DIE PLÄTZE ...

Machen Sie sich bereit, Ihr Datenschutzprogramm zu erstellen oder zu verbessern, indem Sie das Privacy Framework verwenden, um eine solide Grundlage für die Identifizierung und das Management von Datenschutzrisiken zu schaffen.

Identifizieren:

- Identifizieren Sie die Daten, die Sie verarbeiten (z. B. Sammeln, Verwenden, Teilen, Speichern) und bilden Sie deren Fluss durch Ihre Systeme während des gesamten Datenlebenszyklus ab – von der Erfassung bis zur Entsorgung. Dies muss nicht perfekt umfassend sein, vor allem nicht am Anfang, aber es ist eine Grundlage, um Ihre Datenschutzrisiken zu verstehen.
- Führen Sie eine Bewertung des Datenschutzrisikos durch, indem Sie Ihre Datenkarte verwenden, um zu bewerten, wie Ihre Datenverarbeitungsaktivitäten Probleme für Einzelpersonen verursachen könnten (z. B. Verlegenheit, Diskriminierung oder wirtschaftliche Verluste). Bewerten Sie dann die Auswirkungen auf Ihr Unternehmen, wenn Probleme auftreten (z. B. Verlust des Kundenvertrauens oder Reputationsschäden), die sich negativ auf Ihr Endergebnis auswirken können.

- Erkundigen Sie sich nach Optionen für Verträge und die Produkte und Dienstleistungen, die Sie für Ihr Unternehmen verwenden, um sicherzustellen, dass sie Ihren Datenschutzprioritäten entsprechen.

Steuern:

- Die Datenschutzkultur beginnt an der Spitze. Bestimmen Sie, auf welche Datenschutzwerte (z. B. menschliche Autonomie, Anonymität, Würde, Transparenz, Datenkontrolle) sich Ihr Unternehmen konzentriert. Verknüpfen Sie die Datenschutzwerte und Richtlinien Ihres Unternehmens mit Ihrer Datenschutzrisikobewertung, um das Vertrauen in Ihre Produkte und Dienstleistungen zu stärken.
- Kennen Sie Ihre datenschutzrechtlichen Verpflichtungen, damit Sie konforme Produkte und Dienstleistungen entwickeln können.
- Helfen Sie Ihren Mitarbeitern, ihre Rollen und Verantwortlichkeiten zu kennen, damit sie bessere Entscheidungen darüber treffen können, wie sie Datenschutzrisiken bei der Entwicklung und Bereitstellung Ihrer Produkte und Dienstleistungen effektiv bewältigen können.
- Überprüfen Sie regelmäßig, ob sich Ihre Datenschutzrisiken geändert haben. Dies kann der Fall sein, wenn Sie Verbesserungen an Ihren Produkten und Dienstleistungen vornehmen, Ihre Datenverarbeitung ändern oder von neuen gesetzlichen Verpflichtungen erfahren.

„Das Privacy Framework kann ein Marktunterscheidungsmerkmal für das Unternehmen sein, um sein Geschäft ausbauen zu können.
- Mary N. Chaney, Esq., CISSP, CIPP, Direktorin für Informationssicherheit und Datenschutz, ESPERION Therapeutics, Inc.

FERTIG ...

Jetzt, da Sie Ihre Datenschutzrisiken und gesetzlichen Verpflichtungen kennen und über eine Governance-Struktur verfügen, kann sich Ihr Unternehmen auf die Richtlinien und technischen Funktionen für Ihre Systeme, Produkte und Dienste konzentrieren.

Controllieren:

- Sammeln, teilen oder speichern Sie Daten, die Sie nicht benötigen? Überlegen Sie, wie Ihre Richtlinien Ihnen oder anderen Organisationen helfen, die Kontrolle über Daten zu behalten, und wie Einzelpersonen ebenfalls eine Rolle spielen können.
- Berücksichtigen Sie Ihre Datenschutzrisiken und gesetzlichen Verpflichtungen, wenn Sie über die Funktionalität Ihrer Datenverarbeitungssysteme, Produkte oder Dienstleistungen entscheiden. Ziehen Sie ein flexibles Design in Betracht, damit Sie

kostengünstiger auf sich ändernde Datenschutzpräferenzen der Kunden und ein dynamisches rechtliches Umfeld reagieren können.
- Welche Arten der Datenverarbeitung führen Sie durch? Je mehr Sie Daten von Personen und Geräten trennen können, desto größer ist der Gewinn für die Privatsphäre. Überlegen Sie, wie verschiedene technische Maßnahmen wie Anonymisierung, dezentrale Datenverarbeitung oder andere Techniken es Ihnen ermöglichen könnten, die Ziele Ihres Unternehmens oder Ihrer Behörde zu erreichen und gleichzeitig die Privatsphäre zu schützen.

Kommunizieren:

- Erstellen Sie Richtlinien für die interne und externe Kommunikation über Ihre Datenverarbeitungsaktivitäten.
- Erhöhen Sie die Transparenz und das Kundenverständnis, indem Sie klare und zugängliche Hinweise und Berichte bereitstellen oder Warnungen, Nudges oder andere Signale implementieren, um Einzelpersonen über Ihre Datenverarbeitungsaktivitäten und ihre Entscheidungen zu informieren.
- Führen Sie Umfragen oder Fokusgruppen durch, um Ihr Produkt- oder Servicedesign zu informieren? Schließen Sie den Datenschutz ein, damit Sie mehr über die Datenschutzeinstellungen Ihrer Kunden erfahren.
- Überlegen Sie, was Sie im Falle einer Datenschutzverletzung tun werden. Wie werden Sie Benachrichtigungen oder Abhilfemaßnahmen wie Kreditüberwachung oder Einfrieren von Krediten vornehmen?

Schützen:

- Kontrollieren Sie, wer sich bei Ihrem Netzwerk anmeldet und Ihre Computer und andere Geräte verwendet
- Verwenden Sie Sicherheitssoftware, um Daten zu schützen.
- Verschlüsseln Sie vertrauliche Daten, ruhend und während der Übertragung.
- Führen Sie regelmäßige Back-ups der Daten durch.
- Aktualisieren Sie die Sicherheitssoftware regelmäßig und automatisieren Sie diese Aktualisierungen, wenn möglich.
- Verfügen Sie über formale Richtlinien für die sichere Entsorgung von Daten und alten Geräten.

„Wenn Sie ein Datenschutzprogramm einrichten müssen, ist das NIST Privacy Framework ein perfekter Ausgangspunkt.“
- Jeewon Serrato, Partner, BakerHostetler

LOS!

Jetzt ist es an der Zeit, von dort, wo Sie heute sind, dorthin zu gelangen, wo Sie sein

möchten.

- Wie schneidet Ihr Programm im Vergleich zu dem ab, was wir hier vorgeschlagen haben.
- Priorisieren Sie Ihre Zielergebnisse und erstellen Sie einen Aktionsplan.
- Besprechen Sie Ihren Plan als Organisation und nutzen Sie ihn, um auf die Beschaffung von Ressourcen und den Aufbau der Belegschaft hinzuarbeiten, die zum Erreichen Ihrer Ziele erforderlich sind.
- Setzen Sie Ihren Plan in die Tat um! Sie sind auf dem besten Weg, mehr Vertrauen in Ihre Produkte und Dienstleistungen zu schaffen, mit Ihren Partnern und Kunden effektiver über den Datenschutz zu kommunizieren und Ihren Compliance-Verpflichtungen nachzukommen!