

2022 – 2023 DATA PRIVACY COMPLIANCE EXPLAINED:

TIMELINES, CHECKLISTS, CHEAT SHEETS & MORE



This compliance guide is critical for you if your business requires the use of third-party technology to handle high volumes of calls and leads.

Table Of Contents

→ Compliance Regulations

Page 3: Do You Rely on a Third-Party Tech Platform to Handle Your Consumer Calls and Data?

→ STIR/SHAKEN Compliance

Page 4: The Latest on STIR/SHAKEN. How Does It Affect Your Business? What Happens if You or Your Voice Service Provider Are Non-compliant?

Page 5: STIR/SHAKEN Compliance Checklist

→ CCPA/CPRA Compliance

Pages 6-7: What Will the CCPA to CPRA Switch Entail? Who Should Comply With CCPA Regulations? What Happens if Your Organization Is Non-Compliant With CPRA Regulations After Jan. 1, 2023?

Page 8: CCPA/CPRA Compliance Checklist

→ GDPR Compliance

Page 9: What is GDPR? What Happens if Your Organization Is Not GDPR Compliant? Who Should Comply With GDPR?

Page 10: GDPR Compliance Questionnaire & Checklist

→ Developments to Monitor Going Forward

Page 11: Bonus: Timeline for Developments to Monitor in 2023

Page 12: Embracing Regulatory Compliance



Disclosure: The information and materials presented are provided for general informational purposes only and are not intended to be legal advice. The law changes frequently and varies depending on jurisdiction. If you require legal advice, please consult with an attorney licensed to practice in your jurisdiction.

Do You Rely on a Third-party Tech Platform to Handle Your Consumer Calls and Data?

This guide has all the tips and tricks you need to evaluate your current third-party call and lead management service providers and grasp a secure handle over your calls and consumer data.

Refer to this cheat sheet for a detailed look at consumer protection privacy laws and tips on implementing protocols enforced by different regulatory authorities and government agencies.

Protect your business and consumers, stay up to date with compliance mandates, avoid severe monetary penalties, and enhance your company's reputation.



STIR/SHAKEN (Previously the TRACED Act)

- [\[Secure Telephone Identity Revisited \(STIR\) and Signature-based Handling of Asserted Information Using tokens \(SHAKEN\)\]](#)

Many Communications Service Providers (CSPs) are baffled by the recent sequence of reports, orders, and public notices from the Federal Communications Commission (FCC) regarding what CSPs need to do to comply with the STIR/SHAKEN caller ID authentication standards.

STIR/SHAKEN is a framework of interconnected rules and compliance protocols that validate call sources to combat caller ID spoofing on public telephone networks. Companies providing voice services or solutions must implement the protocol to enter the FCC RMDB (Robocall Mitigation Database) and become fully compliant.

- [The Latest on STIR/SHAKEN](#)

On Aug. 5, 2021, the FCC's Wireline Competition Bureau granted a STIR/SHAKEN implementation deadline extension until June 30, 2023, for voice service providers with 100,000 or fewer subscriber lines after finding that these providers may face substantial cost and resource constraints that would prevent STIR/SHAKEN implementation.

- [How Does STIR/SHAKEN Affect Your Business?](#)

Any business making calls to consumers or other businesses could be negatively impacted if its service provider fails to meet and maintain compliance with STIR/SHAKEN.

With the deadline for compliance extended for small voice service providers, here is why your business may have received an extension until 2023:

- You have less than 100,000 lines
- You weren't able to obtain a STIR/SHAKEN token
- A portion of your network does not support Session Initiation Protocol (SIP)

- [What Happens if You or Your Voice Service Provider Are Non-Compliant With STIR/SHAKEN?](#)

If your company makes calls to consumers or other businesses, you can be negatively impacted if your voice service provider fails to meet and maintain compliance with STIR/SHAKEN.

Service providers who fail to meet these requirements may have calls originating on their networks blocked. Being out of compliance may also result in hefty penalties enforced by the FCC.

STIR/SHAKEN Compliance Checklist

- ☐ 1. Register with the FCC
 - ☐ 2. Register with USAC (499 ID)
 - ☐ 3. Obtain an Operating Company Number (OCN) from the National Exchange Carrier Association (NECA)
 - ☐ 4. Submit your application to an approved certification authority
 - ☐ 5. Confirm your filing and complete implementation of STIR/SHAKEN with the FCC Robocall Mitigation Database
- **Implementation timeline:** Receiving STIR/SHAKEN compliance is a five-step process that can take up to one year.



CCPA (Soon-to-Be CPRA)

[California Consumer Privacy Act]

As the switchover from **CCPA** to CPRA (California Privacy Rights Act) approaches, a significant portion of California-based companies remain uncertain about what changes will be imposed starting on Jan. 1 of 2023.

• What Will the CCPA to CPRA Switch Entail?

Essentially, the CPRA was established to serve as an added layer of protection to the landmark CCPA. Here's a breakdown of what the switchover will look like:

California Consumer Protection Act Established in 2018	California Privacy Rights Act Established in 2020	CCPA & CPRA Together January 1, 2023
<ul style="list-style-type: none">• The landmark privacy regulation in the United States with the initial intent to create transparency, not to enforce privacy• Companies must provide privacy disclosures and notices for data collection, use, sharing, and selling• 45-day grace period for Data Subject Asset Request (DSAR)• Covered third-party contracts• Explicit consent for collecting and selling a minor's data	<ul style="list-style-type: none">• Covers all CCPA requirements• Explicit consent for the collection and use of sensitive data• Data protection assessments for high-risk activities• Right to restrict the processing of sensitive information in any form• Data retention enforced: only keep data only as long as it's needed	<ul style="list-style-type: none">• Enforce all CCPA and most CPRA requirements• Identify the adequate data protection and security controls for personal data• Evaluate a company's privacy, security, and compliance practices• Ensure consumers have the right to opt-out of targeted advertising and automated decision-making

CCPA (Soon-to-Be CPRA)

• Who Should Comply With CCPA Regulations?

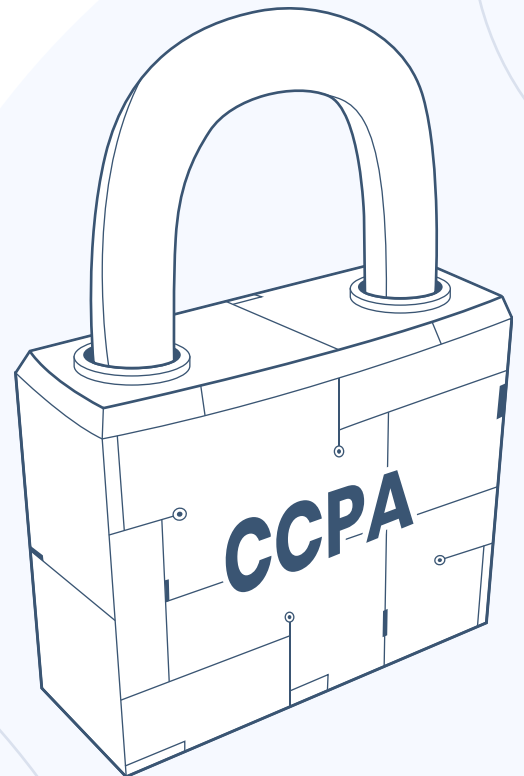
- Businesses with gross annual revenue of \$25 million in the preceding calendar year*
- Businesses that buy, receive, or sell the personal information of 100,000 or more California consumers, households, or devices for commercial purposes.
- Businesses that get 50% or more of their annual revenue from:
 - Selling or sharing California residents' personal information;
 - Sharing consumer's personal information for cross-content behavioral advertising.

• What Happens if Your Organization Is Non-Compliant With CPRA Regulations After Jan. 1, 2023?

Non-compliant companies risk the following statutes, among other repercussions:

- ! A penalty of up to \$2,500 per violation;
- ! A penalty of up to \$7,500 per intentional violation of the statute;
- ! The CPRA will permit a new penalty of up to \$7,500 for violations (even if unintentional) of the consumer privacy rights of minors.

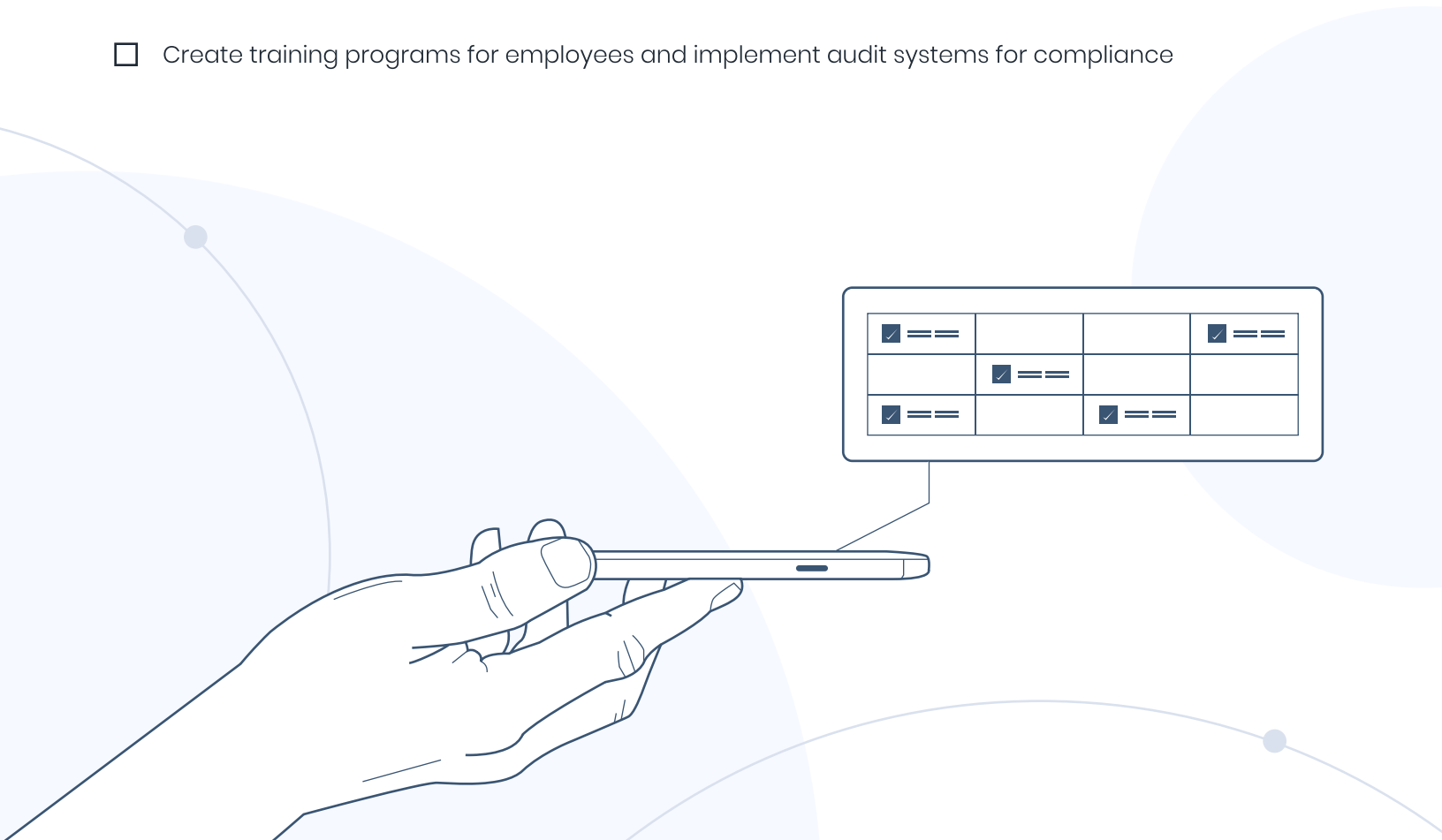
*Mandatory compliance doesn't apply to nonprofits or government agencies but may apply to the vendors that provide services to nonprofits or government agencies.



CCPA/CPRA Compliance Checklist

- Complete the following steps to attain compliance.

- ☐ Determine if the CCPA applies to your business
- ☐ Determine if data you collect qualifies as “personal information”
- ☐ Determine if your business should stop selling consumer data
- ☐ Update your privacy policy and implement security procedures to stay current with CCPA-related practices, including how personal information is collected, how personal information is handled
- ☐ **Example:** Collection Notices, Opt-Out Right Notices, Financial Incentive Notices, and Privacy Policy
- ☐ Enable systems holding personal information about California residents to receive and process sales opt-in and opt-out requests
- ☐ Make sure pricing models, and business practices comply with non-discrimination requirements enforced by the CCPA
- ☐ Create training programs for employees and implement audit systems for compliance



A line drawing of a hand holding a smartphone. A callout box points to the phone, containing a 3x3 grid of checkboxes. The grid is as follows:

<input checked="" type="checkbox"/> ==			<input checked="" type="checkbox"/> ==
	<input checked="" type="checkbox"/> ==		
<input checked="" type="checkbox"/> ==		<input checked="" type="checkbox"/> ==	

GDPR (Applicable to the European Union)

[General Data Protection Regulation]

With 94% of the EU-based surveyed companies being unprepared and out of compliance with GDPR privacy regulations, there is a clear need for organizations to forgo error-prone manual processes in favor of automating their privacy programs.*

Under GDPR, organizations are obligated to respond to a data subject's or consumer's request about their personal data. The regulation applies to any person, business, or organization that collects, handles, or processes the personal data of any person living in the European Union.

Who Should Comply With GDPR?

Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU.

- What Happens if Your Organization Is Not GDPR Compliant?

Non-compliance can expose companies to operational vulnerabilities and severe penalties, including: Fines up to €10 million or 2% of the non-compliant company's global annual revenue for low-level violations (the greater amount determines how much the company is fined) Doubled penalties for high-level violations, with fines up to €20 million or 4% of the company's global annual revenue (the greater amount criteria also applies to high-level violations).



* Source: CYTRIO State of CCPA & GDPR Privacy Rights Compliance Research Report, Q2 2022.

GDPR Compliance Questionnaire & Checklist

The following questions cover the five general areas of GDPR compliance.*

- Lawful Basis and Transparency

- ☐ Do you conduct an information audit to determine what information you process and who has access to it?
- ☐ Does your privacy policy provide clear information about your data processing and legal justification?

- Data Privacy

- ☐ Do you encrypt, pseudonymize, or anonymize personal data whenever possible?
- ☐ Does your organization have an internal security policy for team members? Do you build awareness about data protection?
- ☐ Do you regularly conduct a data protection impact assessment? What does your process entail?
- ☐ Do you have a process in place to inform authorities and data subjects about any possible data breaches?

- Accountability and Governance

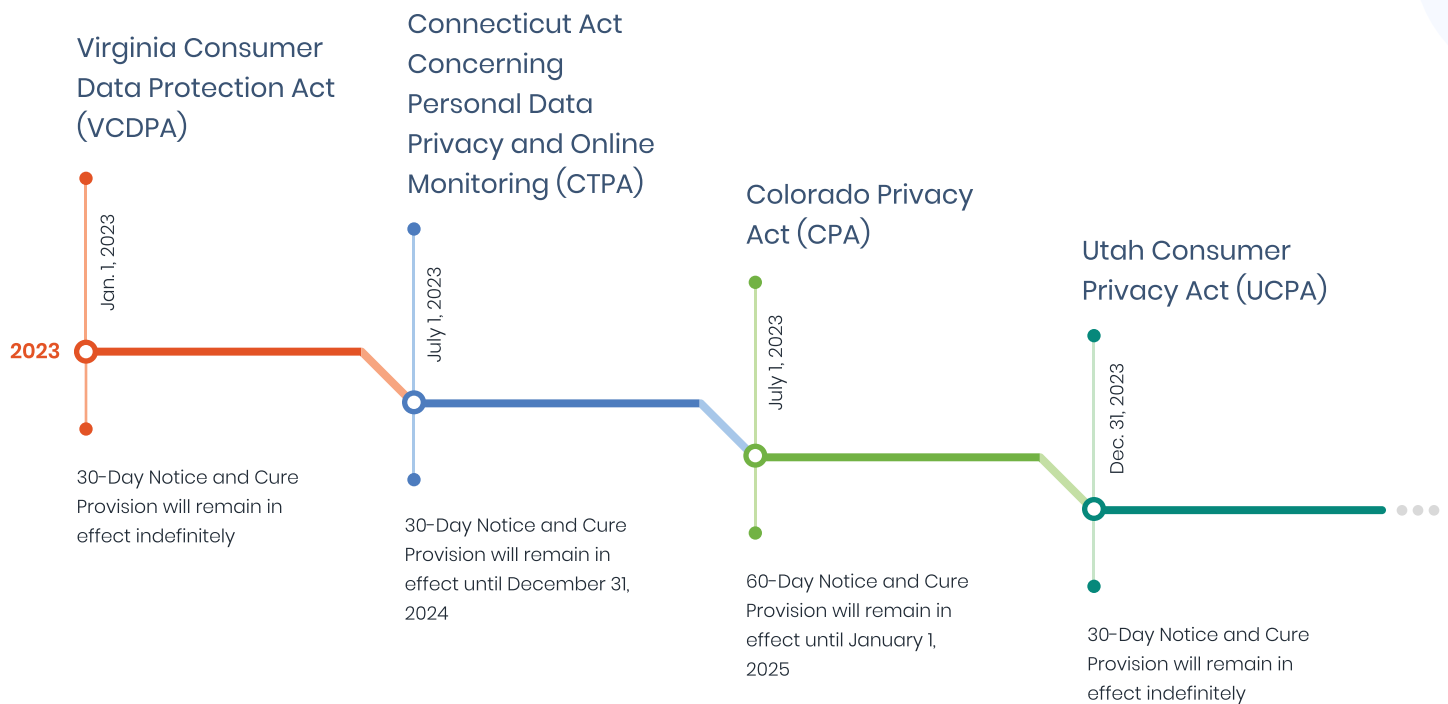
- ☐ Do you have a designated person in your organization responsible for ensuring GDPR compliance?
- ☐ Do you sign data processing agreements with third parties that process personal data on behalf of your organization?

- Privacy Rights

- ☐ Have you made it easy for your customers to request and receive all the information you have on them?
- ☐ Do you have a simple process to allow your customers to correct or update their personal information?
- ☐ Do you have a system that allows consumers to get their information removed?

Bonus: Timeline for Developments to Monitor in 2023

Looking ahead to 2023 and beyond, more consumer privacy laws and regulations will surface in the United States. The following compliance laws will go into effect in 2023:



Next Steps: Embracing Regulatory Compliance

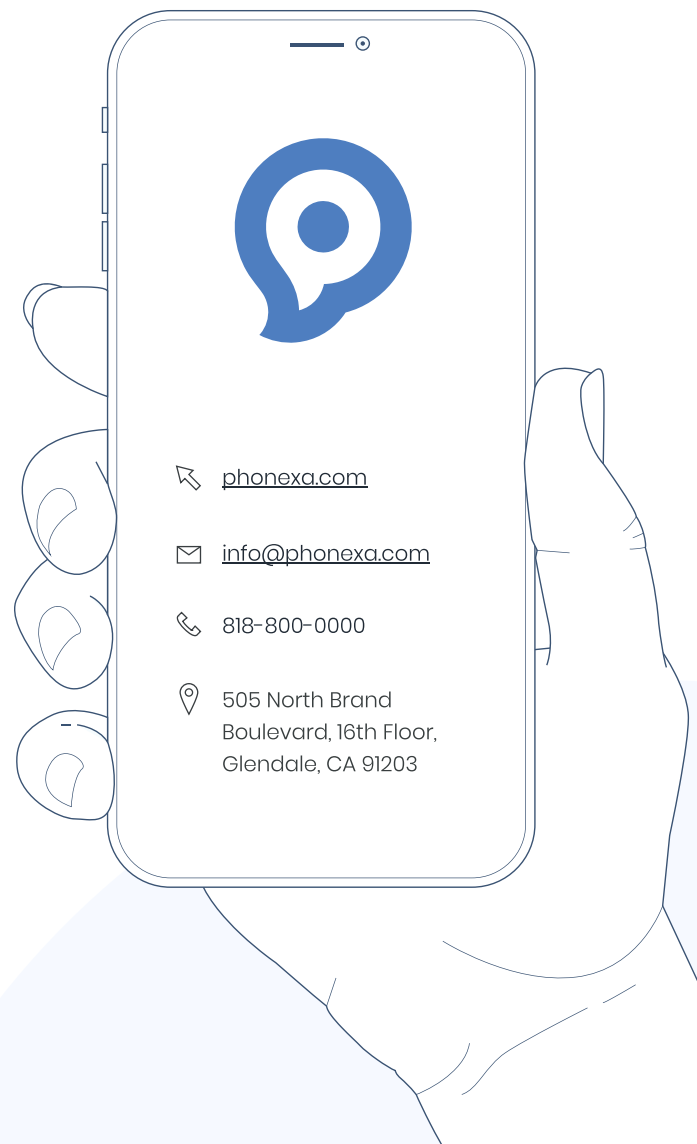
With new and updated consumer protection laws being rolled out in full force, organizations handling consumer data must embrace the power of local, national, and international regulations by implementing proactive compliance strategies in their organizations.

Crucial Next Steps:

- Evaluate your current third-party technology for compliance.
- Seeing compliance gaps? It's time to consider a compliant provider.
- We're right here. Phonexa acts in accordance with all of the **compliance** regulations mentioned in this handbook – and more.

Follow the **Phonexa blog** to stay current and receive more content and tips on consumer privacy laws and regulations affecting the marketing automation industry today.

Phonexa is a performance marketing software and all-in-one marketing automation solution for calls, leads, clicks, email, SMS, accounting, and more. The company powers direct advertisers and lead generators alike across all businesses and industries by optimizing inbound web and call campaigns, and outbound call, email, and SMS campaigns – all while having the ability to enhance the consumer journey along every step of the way. Complete with a suite of turnkey marketing products and solutions, Phonexa's customizable tools are uniquely designed to maximize workflow efficiency and revenue. Phonexa has the scalability, tools, and partnerships to serve clients across industries, especially those with high consumer demand products and services. The company is headquartered in Los Angeles with additional offices in the United Kingdom and Ukraine. For more information, please visit www.Phonexa.com.



[Schedule a consultation](#)