Contact Center Compliance Handbook

Level 9, 1 Chandos Street
St Leonards, NSW 2065, Australia
info@contactspace.com
contactSPACE
www.contactspace.com

Contents

1.0 Introduction 03
2.0 TCPA 04
3.0 FDCPA 06
4.0 HIPAA 08
5.0 21st Century Cures Act 10
6.0 California Consumer Privacy Act (CCPA) 12
7.0 Privacy Shield 13
8.0 EU GDPR 15
9.0 UK GDPR (DATA PROTECTION ACT) 17
10.0 Reducing Scam Calls Industry Code 19
11.0 The Spam Act 20
12.0 The Privacy Act 22
13.0 SOC 2 Certification 24
14.0 Payment Card Industry Data Security Standard 26
15.0 ISO 27K 28
16.0 SIG 30
17.0 Data Isolation & Single Tenant Architectures 31
18.0 Using Skills for Compliance 32
19.0 Conclusion 33

Introduction

One of the most challenging areas of operating a contact center is balancing the need to remain in compliance with government regulation and best practice, against controlling costs and obtaining the best productivity possible for your business. Improving your contact strategies whilst meeting outbound dialing regulations remains a key area of concern for many contact centers.

Legislation, regulation, and the courts are continuing their efforts to make it more difficult to include mobile telephone numbers in automated dialing campaigns. Registers of numbers that cannot legally be dialed have been implemented globally. The availability of Caller ID as an industry standard makes it even easier to screen unwanted calls.

There is a need for external regulation. Despite decades of attempts at industry self-regulation, it has been repeatedly shown that legislation in law remains the most powerful tool that can be used to enforce compliance to an acceptable standard. While industry self-regulation is intended to ensure that businesses operate in a safe, competent, and ethical manner, it has been repeatedly observed that in practice, it falls short of the protections expected by the general populace. This is typically when legislation in law and mandated protection of consumer rights becomes important.

Healthcare client data privacy regulations continue to be modified across the globe.

In the US, HIPPA is a privacy standard that has been adopted, specific to the health industry. Australia governs health industry privacy standards under an all-encompassing privacy act. The European Union and the UK do the same, with their EU GDPR and UK GDPR legislation.

Outside of healthcare data, globally, many nations and unions have chosen to legislate rules on consumer protections and client data privacy. The most well-known, GDPR, is one of the widest ranging pieces of legislation passed by a governing body in history.

Restrictions on contacting clients who do not wish to be contacted, or who have withdrawn consent, have also been strengthened. In the US, the FTC Telemarketing Sales Rule applies. In Australia, it is the Spam Act of 2008.

At local and regional levels, consumer data privacy is also addressed, particularly in nations where federal law cannot or will not legislate.

The US is currently in the process of considering Federal Privacy legislation.

Typically, a regional government passing legislation creates a waterfall effect on other legislatures following suit. In 2018, the US state of California introduced the California Consumer Privacy Act. In extension, the state of Virginia passed the Consumer Data Privacy Act in March 2021, and the state of Colorado enacted the Colorado Privacy Act in July 2021.

The protections in law which have been legislated globally typically carry some formidable penalties for breaches. In 2020, British Airways was fined £22 million (USD$26 million) for GDPR non-compliance.

It doesn't stop there. WhatsApp was fined £225 million in 2021, and the list of organizations receiving fines issued that are in the millions of dollars continues to grow to nearly one thousand. In fact, the total amount of all GDPR fines issued since late 2018, when the legislation came into effect, is over €1.29 billion.

When considering payment card compliance, the PCI-DSS standard is used by card merchants to enforce it. To keep you in compliance to an acceptable standard, pcipayspace is our innovative payment processing solution. It enables you to get on with what's important – taking payments efficiently, maximizing your conversion rates, and minimizing IVR abandonment.

contactSPACE solutions have been designed and built to help you deliver effective business outcomes while easily managing compliance risk. Organizations use contactSPACE to deliver an outstanding customer and agent experience, while remaining in compliance with all relevant legislatures.

TCPA

What is it?

The Telephone Consumer Protection Act 47 U.S.C 227 (TCPA) was introduced by the US Federal government to regulate calls citizens received – specifically, reducing unwanted calls.

The TCPA has a number of restrictions on Automated Telephone Dialing Systems (ATDS). Previously, there has been a significant amount of confusion as to what exactly an ATDS is. However, in April 2021, the Supreme Court deemed that for a device to qualify as an ATDS, it must be based on the capacity to store or produce numbers from a random or sequential generator. The case ruled that an automatic system that may phone a user from a stored number but otherwise not generated in a random or sequential way (such as how two-factor authentication works) does not meet this definition under the TCPA.

Under this interpretation of the law, certain TCPA rules may not apply, even if using predictive dialing, provided you're calling a list of customers, rather than randomly or sequentially generated numbers. However, the legislation still imposes significant restrictions on outbound calling, meaning that TCPA compliance is extremely important for US-based businesses in particular.

> TCPA compliance is extremely important for US-based businesses in particular

TCPA rules state:

- You cannot call residences before 8 a.m. or after 9 p.m., according to the recipient's time zone.
- Companies must maintain an internal "do-not-call" list, and anyone upon that registry may not be called. Requests to not be called must be honoured for five years.
- Solicitation calls may not be made to anyone on the National Do Not Call Registry.
- Callers must provide their name, the name of the business they represent, and a telephone number or address where the recipient can contact that business.
- When predictive dialing, you must not go above a 3% abandonment rate for each campaign over a 30-day period.
- Solicitation calls may not use an artificial voice or recording.
- Automated Telephone Dialing Systems (ATDS) may not dial up emergency phone numbers, hospital emergency numbers, a physician's office, health care rooms, a cell phone, or any instance where the recipient is charged for the call.
- You cannot send texts or make telemarketing calls to cell or smartphones (mobile phones) without prior express written consent.
- Calls to collect a debt are not considered telemarketing calls – be sure to have prior express written consent if calling a mobile phone of any kind.
- If the call contains no solicitation for money, goods or services, a call to a residential telephone is still prohibited if placed by way of ATDS dialer.

Some calls are not restricted by TCPA. Generally, these are not-for-profit type calls.

What businesses does this apply to?

- Any businesses in the United States.
- Any business calling US customers.

TCPA (Cont.)

The TCPA extends to all facets of outbound telephone contact, including but not limited to autodialed and manual phone calls, faxes, voice messages (both organic and automated), text messages and automatic dialing systems.

What does it cost the business to achieve?

Component	Cost	Time
TCPA gap assessment	$20,000 – $30,000	2 weeks full time internal team
Complete TCPA audit	$20,000 – $50,000	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

Mandatory?

Yes.

What regions does this apply to?

United States.

What will non-compliance cost our business?

The financial penalties for failure to comply with the TCPA can be immense. TCPA violations can result in fines being levied of USD$500 per instance, with wilful violations being tripled up to USD$1500 per instance.

Calling a list with 100 records outside of TCPA compliance could result in fines of USD$50,000, or USD$150,000 if found to be an aggravated offence.

While consumers may have been filing fewer TCPA lawsuits, they were complaining more in 2018 than they did in 2017. The number of complaints filed with the Consumer Financial Protection Bureau was 6% higher in 2018 than 2017, and the number of complaints registered by the Better Business Bureau was 11% higher last year than the number from 2017.

How can contactSPACE solutions assist with this requirement?

contactSPACE enables you to ensure TCPA compliance, without compromising the effectiveness of your outbound dialing campaigns. We also help US-based organizations make efficient, compliant outbound calls using Twilio Flex and Amazon Connect, with our 4flex and 4connect solutions respectively.

Using contactSPACE, you have complete control to automatically define who you call, when you call them, and how you call them, ensuring you maintain compliance. You can do this while still ensuring that you contact a given record at the right time in the sales funnel, maximizing their propensity to convert.

For example – you can automatically define your dialing mode for each given interaction, depending on the number you're dialing, and your interaction history with the customer. You may wish to only predictively dial a customer's landline number, to ensure compliance. If the call is not answered, you might like to try their mobile number using preview or progressive dialing on the second and third attempts.

FDCPA

What is it?

The Fair Debt Collection Practices Act, Pub. L. 95-109; 91 Stat. 874 (US Federal Law) provides legal protection for consumers from abusive debt collection practices.

- The Act creates legislates guidelines under which debt collectors may conduct business and defines the rights of consumers involved with debt collection.
- Applies to third party collectors, rather than the ''original creditor''.
- Debts purchased by a collection company do not trigger the statutory definition of a ''debt collector'' under FDCPA (Henson vs Santander Consumer USA Inc 2017).
- Debts purchased by a collection company who solely purchased debt may be subject to FDCPA legislation.
- The Act defines what you can and cannot do when soliciting settlement of a debt.

What businesses does this apply to?

- US-based businesses.
- Businesses serving US clients.
- Third-party debt collectors, such as those who work for a debt collection agency. Credit card debt, medical bills, student loans, mortgages, and other kinds of household debt are covered by this law.

Mandatory?

Yes, for the businesses described above.

What regions does this apply to?

United States.

What does it cost the business to achieve?

It is highly likely that a business that is required to comply with FDCPA must also comply with GDPR or TCPA. As such, many business controls, like management of the outbound dialer, may already be operating in a mostly FDCPA compliant manner. There may be little work for the business to address FDCPA compliance requirements in extension to GDPR or TCPA.

For a business without any other form of compliance and starting from having few processes in place, the following costs could be considered:

Component	Cost	Time
TCPA gap assessment	$20,000 – $30,000	2 weeks full time internal team
Complete TCPA audit	$20,000 – $50,000	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

FDCPA (Cont.)

What will non-compliance cost our business?

The FDCPA is a strict liability law, which means that a consumer need not prove actual damages to claim statutory compensation of up to $1,000 plus reasonable attorney fees if a debt collector is proven to have violated the FDCPA.

The most common violations of the FDCPA include:

- Attempting to collect a debt not owed.
- Illegal communication tactics.
- Excessive phone calls.

How can contactSPACE solutions assist with this requirement?

contactSPACE allows you to restrict your dialing campaigns and initiatives to a time of day that is compliant with this legislation. In addition:

- Your dialing list can be configured with filtering rules, which you can use to ensure that your call center only reaches people you'll allowed your team to get in touch with at any given moment.
- contactSPACE CallGuides ensure that your agents identify themselves to the consumer correctly.
- Our call recording and quality assurance tools ensure that your agents are providing the correct disclaimers/information to debtors, and not making misrepresentations to the people they are calling. You can also use contactSPACE speech analytics to automatically check compliance with regards to what your agents are saying on each call.
- You can modify your contact strategies to limit how many times you contact a given person or phone number, either during a specific time window, or with regards to overall attempts. Meaning, no more worrying about accidentally contacting someone too many times.
- contactSPACE allows you to minimize the number of outbound calls you need to make, reducing compliance risk while still ensuring excellent collections results. For example, you can use contactSPACE Intellicast to broadcast SMS reminders to debtors, and have them call the number displayed to make a repayment over IVR, without a phone call ever having to take place.

HIPAA

What is it?

HIPAA is the health Insurance Portability and Accountability Act 1996. The Act establishes a set of national standards for the protection of certain health information.

What businesses does this apply to?

- Healthcare services and providers.
- Payment processors for health services.
- Health plan and funds.
- Health care clearinghouses.
- Any health care provider who transmits health information in electronic form in connection with transactions for which the United States Secretary of Health and Human Services has adopted standards under HIPAA (the “covered entities”).
- Business associates and contractors of health providers.

For help in determining whether you are covered, use the Centers for Medicare & Medicaid Services’ decision tool.

The US Office for Civil Rights (OCR) enforces the Privacy and Security Rules in several ways:

- Investigating complaints filed with it.
- Conducting compliance reviews to determine if covered entities comply.
- Performing education and outreach to foster compliance with the Rules.

The OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

Mandatory?

Yes, for organizations providing the above services to US-based patients.

What regions does this apply to?

- Global, when servicing US-based patient data.
- Outside of the US, HIPAA may be used as a best practice in the absence of effective local regulatory frameworks.

What does it cost the business to achieve?

Medium sized organizations may assume up to two years to define scope, interview human resources, create workflows and manage change.

For smaller organizations that only have an individual location, with a full-time staff member devoted to HIPAA, it could take a typical office less than 6 months to become compliant.

HIPAA software and process audits may incur charges of up to $150 per hour to assess for compliance.

HIPAA (Cont.)

Component	Cost	Time
HIPAA Gap Assessment	$20,000 – $30,000	2 weeks full time internal team
Complete HIPAA Audit	$20,000 – $50,000	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

What will non-compliance cost our business?

HIPAA rules do not have any private cause of action (sometimes called "private right of action") under US federal law. While it is against US law for medical providers to share health information without the patient's permission, federal law prohibits filing a lawsuit asking for compensation.

The US Office for Civil Rights may refer non-compliance incidents to the US Department of Justice (DoJ) for criminal investigation.

The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision.

How can contactSPACE solutions assist with this requirement?

- contactSPACE can help you to restrict agent access to protected systems. Agents get only the information they need to complete their duties, leaving your contact center 100% compliant.
- Agent scripting and workflow tools are used so that agents can enter data into your datastore, without having access to unnecessary areas of protected client data.
- contactSPACE includes preferred contact number fields, ensuring that your team don't accidentally call a protected location, like a place of employment.

21st Century Cures Act

What is it?

If a business or person is engaged in biomedical, behavioral, clinical, or other research, in which identifiable, sensitive information is collected, they must implement policies and mechanisms for appropriate secure data sharing across systems that include protections for privacy and the security of data.

Any data and information sharing must be undertaken in accordance with any other applicable privacy laws and regulations.

Businesses who fail to comply may be levied with penalties of up to $1,000,000 per violation.

What is unusual about it?

This legislation has broadened its initial scope – it originally related to businesses being required to stop information blocking within the industry. As with many acts of legislature, riders have been added which address privacy for medical clients and subjects. This extends to management of health records.

> ***"The Cures act is an unusual piece of legislation in terms of how universally it was accepted... it affected mostly the National Institutes of Health and the Food & Drug Administration (FDA), but the many moving parts involving such issues as the opioid crisis and mental health make the impact broader than anyone originally thought it would be. It's a very important piece of legislation that has not yet been deeply explored."***
>
> **Fran Miller**
>
> Professor emeritus who has taught a seminar on food and drug law at the Boston University School of Law since 2003.

What businesses does this apply to?

- Healthcare services and providers.
- Payment processors for health services.
- Health plan and funds.
- Health care clearinghouses.
- Any health care provider who transmits health information in electronic form in connection with transactions for which the United States Secretary of Health and Human Services has adopted standards under HIPAA (the "covered entities").
- Business associates and contractors of health providers.

The US Office of the National Coordinator for Health IT (ONC) enforces the 21st Century Cures Act in several ways:

- Investigating attestations filed with it.
- Conducting compliance reviews to determine if covered entities comply.
- Performing education and outreach to foster compliance with the Act.

ONC also works in conjunction with the Department of Justice (DoJ) to investigate possible criminal violations of HIPAA.

Mandatory?

Yes. To organizations providing the above services to US-based patient data.

The Centers for Medicare and Medicaid (CMS) requires their healthcare providers to attest annually whether they have blocked health information. Attestations indicating information blocking will be publicly reported on the CMS Care Compare site.

What regions does this apply to?

- Global, when servicing US-based patient data.
- Outside of the US, the Act may be used as a best practice in the absence of effective local regulatory frameworks.

21st Century Cures Act (Cont.)

What does it cost the business to achieve?

Organizations must attain or retain certification with accredited certification bodies using ONC criteria for health information technology.

Medium sized organizations may take up to two years to define scope, interview human resources, create workflows and manage change.

For smaller organizations that only have an individual location, with a full-time staff member devoted to 21st Century Cures Act, it could take a typical office less than 6 months to become compliant.

21st Century Cures Act software and process audits may incur charges of up to $150 per hour to assess for compliance.

Component	Cost	Time
21st Century Cures Act gap assessment	$20,000 – $30,000	2 weeks full time internal team
Complete 21st Century Cures Act audit	$20,000 – $50,000	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

What will non-compliance cost our business?

Electronic health record vendors and other developers must attain or retain certification with accredited certification bodies using ONC criteria for health information technology. These vendors will need to provide assurances to healthcare organizations that they are not exposed to information blocking through having a business relationship with them.

There are various deadlines for each of the CEHRT component criteria. The first compliance date is December 31, 2022, and enforcement of certification by the ONC is expected to commence thereafter.

How can contactSPACE solutions assist with this requirement?

- Your contactSPACE solution can restrict agent access to protected systems. Agents get only the information they need to complete their duties, leaving your contact center 100% compliant.
- Agent scripting and workflow tools are used so that agents can enter data into your datastore without having access to unnecessary areas of protected client data.
- contactSPACE includes preferred contact number fields, ensuring that your team don't accidentally call a protected location, like a place of employment.

California Consumer Privacy Act (CCPA)

The US state of California passed the California Consumer Privacy Act on 28 June 2018, taking effect on 1 January 2020. This law grants rights to transparency and control over the collection of personal information by companies in a similar means to GDPR.

Critics have argued that such laws need to be implemented at the federal level to be effective, as a collection of state-level laws would have varying standards that would complicate compliance.

Two other US states have since enacted similar waterfall legislation: Virginia passed the Consumer Data Privacy Act in March 2021 and Colorado enacted the Colorado Privacy Act in July 2021.

What businesses does this apply to?

- All organizations serving California residents and having at least USD$25 million in annual revenue.
- Organizations serving California residents that have personal data of at least 50,000 people.
- Organizations that collect more than half their revenue from the sale of California residents' personal data.

Mandatory?

Yes, if your business meets at least one of the criteria listed above.

What regions does this apply to?

- Organizations holding or contacting personal data of California residents.
- The Attorney general of California reported that up to 75% of Californian businesses will be expected to comply with this legislation.

What does it cost the business to achieve?

- Ongoing compliance costs have been estimated at around USD$6,300 per year.*
- Businesses with less than 20 employees may experience costs of around USD$20,000 to achieve compliance.
- Businesses with more than five hundred employees may pay around USD$2 million in set up costs.

Component	Cost	Time
CCPA Standardized regulatory assessment	$20,000 – $30,000	2 weeks full time internal team
Complete HIPAA audit	$20,000 – $50,000	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

*Source: www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion

Privacy Shield

What is it?

The EU-US and Swiss-US Privacy Shield Frameworks were designed by the US Department of Commerce and the European Commission and Swiss Administration. Privacy Shield aimed to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States, in support of transatlantic commerce.

Following a landmark ruling, The EU-US Privacy Shield Framework can no longer be relied on to provide evidence of compliance with the GDPR (Judgement of the Court of Justice of the European Union in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems).

What businesses does this apply to?

- No longer applies. Superseded by EU enforceable standard contractual clauses (SCCs) and GDPR.

Prior to July 2020, it applied to:

- Organizations operating in the United States with a need to transfer client personal data to Europe or Switzerland.
- Organizations operating in Europe with a need to transfer client personal data to the United States or Switzerland.
- Organizations operating in Switzerland with a need to transfer client personal data to the United States or Europe.
- Any organization transferring client personal data between the US and Europe or between the US and Switzerland.

Mandatory?

No. As of July 2020, Privacy Shield is no longer a valid lawful basis on which to transfer personal data from the EU to the United States. The US Department of Commerce has expressed deep disappointment in the invalidation but is willing to work with the EU Commission and Data Protection Board.

What regions does this apply to?

- United States.
- European Union.
- Switzerland.
- Australia was not a party to the EU-US Privacy Shield. It also does not have EU adequacy status. This is because the Australian Privacy Act does not apply to small businesses, employee data, and political parties, amongst others.

What did it cost the business to achieve?

Organizations must attain or retain certification with accredited certification bodies using ONC criteria for health information technology.

Medium sized organizations may take up to two years to define scope, interview human resources, create workflows and manage change.

For smaller organizations that only have an individual location, with a full-time staff member devoted to 21st Century Cures Act, it could take a typical office less than 6 months to become compliant.

21st Century Cures Act software and process audits may incur charges of up to $150 per hour to assess for compliance.

Privacy Shield (Cont.)

Component	Cost	Time
Privacy Shield gap analysis	$20,000 – $30,000	2 weeks full time internal team
Complete onsite assessment	$20,000 – $50,000	2 weeks full time internal team
Remediation and retesting	$10,000	Up to 6 weeks
Legal	$10,000	2 weeks spread out over 3 months
Report on Compliance (ROC) submission and certification	Up to $3,250	
Build vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

What will non-compliance cost our business?

A former certification called Safe Harbor was superseded by the Privacy Shield.

Courts have found that Safe Harbor and Privacy Shield are still an ineffective means of handling data.

Now that Privacy Shield has been found to be inadmissible in court, the EU is relying on standard contractual clauses (SCCs) to safely approach data transfer from the European Economic Area (EEA).

How can contactSPACE solutions assist with this requirement?

- Requirement no longer active, compliance will rest under EU-US GDPR, US-SW GDPR or UK GDPR.

EU GDPR

What is it?

The General Data Protection Regulation. A regulation in European Union law on data protection in the EU and the European Economic Area (EEA).

GDPR forbids the transfer of the personal data of EU data subjects to countries outside of the EEA — known as third countries — unless appropriate safeguards are imposed, or the third country's data protection regulations are formally considered adequate by the European Commission (Article 45).

As EU GDPR is a regulation, it is legally binding and applicable to contact centers, as contact centers are considered data controllers. Data controllers must disclose any data collection to an EU resident at the time of collection, declare the basis of data collection, and declare how long it will be stored for. If any client data is to be shared with a third party, this must be disclosed, in addition.

The principle that processing is prohibited but subject to the possibility of authorization also applies to the personal data which is used to send e-mails and SMS, as well as making phone calls. Processing is only allowed by the General Data Protection Regulation (GDPR) if either the data subject has consented, or there is another legal basis, such as "legitimate interest". This also applies to call recordings – a typical disclaimer is not considered sufficient to gain assumed consent to record calls.

Adopted in 2016 and became enforceable in May 2018.

What businesses does this apply to?

- Any EU organizations that hold EU resident personal information.
- Any organization in a third country that serves, holds or maintains EU resident records.
- Organizations outside of the EU that wish to obtain a stronger competitive advantage.
- Organizations seeking structure on the design of internal controls for their service organization.
- A business seeking peace of mind.

Mandatory?

Yes, excepting personal or household activities, law enforcement or national security purposes.

What regions does this apply to?

GDPR applies to organizations conducting business in the European Union or the European Economic Area.

Further, the regulation has become a model for many national laws outside of the EU:

- Turkey
- Mauritius
- Chile
- Japan
- Brazil
- South Korea
- Argentina
- Kenya

As EU GDPR is a regulation, it is legally binding and applicable to contact centers, as contact centers are considered data controllers.

EU GDPR (Cont.)

What does it cost the business to achieve?

Component	Cost	Time
Readiness assessment	Productivity loss of dedicated team	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

What will non-compliance cost our business?

Violations of data transfer under GDPR can result in fines or penalties from a regulator of up to approximately $24 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

H&M was fined £35 million, and Google was fined £50 million in 2020 for GDPR breaches.

How can contactSPACE solutions assist with this requirement?

- Unless a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so.
- Using contactSPACE, you can define different contact strategies based on the level of consent you received have to get in contact. For example, hot leads who have given express consent to be called will go straight to the front of the calling queue, while leads with a lower level of implied consent won't be placed in the calling funnel.

UK GDPR (DATA PROTECTION ACT)

What is it?

UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018. The Data Protection Act was the UK's implementation of the EU General Data Protection Regulation (GDPR).

The applicability of EU GDPR in the United Kingdom was affected by Brexit, but the regulation under the EU, known as EU GDPR, will be modified, and referred to as "UK GDPR".

The UK will not restrict the transfer of personal data to countries within the EEA under UK GDPR. However, the UK will become a third country under the EU GDPR, meaning that personal data may not be transferred to the country unless appropriate safeguards are imposed.

As UK GDPR is a regulation, it is legally binding and applicable to contact centers, as contact centers are considered data controllers. Data controllers must disclose any data collection, declare the basis of data collection, and declare how long it will be stored for. If any client data is to be shared with a third party, this must be disclosed, in addition.

Companies operating outside of the UK and EU have invested heavily to align their business practices with GDPR. The area of GDPR consent has several implications for businesses who record calls as a matter of practice. A typical disclaimer is not considered sufficient to gain assumed consent to record calls.

What businesses does this apply to?

- Any UK business that has access to client identifying data.
- Any non-UK business that holds data on UK residents or transfers data from the UK to a third country.

Mandatory?

Yes, excepting personal or household activities, law enforcement or national security purposes.

What regions does this apply to?

Organizations conducting business in the UK.

UK GDPR (DATA PROTECTION ACT) (Cont.)

What does it cost the business to achieve?

Component	Cost	Time
Readiness assessment	Productivity loss of dedicated team	2 weeks full time internal team
Legal	£10,000	2 weeks spread out over 3 months
Build vs buy decisions	£5 – £50k depending on mix of commercial and DIY	2 months
Staff training	£5,000	1 week
Auditor	£17,000	1 month
Project lead	£75,000	6 months
Tools	£30,000	N/A
Data Protection Fee (payable to the Information Commissioners Office	The fee can be up to £2,900 for businesses who employ more than 250 staff and have an annual turnover of above £36 million.	ico.org.uk/for-organizations/how-much-will-i-need-to-pay/

What will non-compliance cost our business?

Violations of data transfer under UK GDPR can result in fines or penalties from a regulator of up to approximately £17.5 million or 4% of the total global annual turnover of the preceding financial year, whichever is higher.

How can contactSPACE solutions assist with this requirement?

- Unless a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so.
- Using contactSPACE, you can define different contact strategies based on the level of consent you received have to get in contact. For example, hot leads who have given express consent to be called will go straight to the front of the calling queue, while leads with a lower level of implied consent won't be placed in the calling funnel.

Reducing Scam Calls Industry Code

What is it?

The Australian Communications Alliance is implementing the Reducing Scam Calls Industry Code (C661:2020) in order to identify, track, block and disrupt scam calls.

According to Section 4.2.1 of the Industry Code, a telecommunications operator can only originate calls on its network with Caller IDs using the phone numbers it has been allocated.

In November 2021, Telstra will start blocking calls from Twilio originating on networks in Australia that have:

1. Outgoing and Verified Caller-ID Phone Number: Telstra Phone Number (rather than a Twilio Phone Number).
2. To Phone Number: Telstra Phone Number.

This restriction only applies to calls from Telstra-held Australian Caller IDs to Australian Phone Numbers. If you use Twilio Phone Numbers for making calls to Australian Phone Numbers, these calls won't be affected.

Other operators in Australia may also begin implementing the Industry Code in the near future.

Please review the Voice Call Guidelines for Australia to understand the voice call restrictions and best practices.

What businesses does this apply to?

All businesses using Twilio.

Mandatory?

No.

What regions does this apply to?

Australian numbers dialed on the Twilio network.

What does it cost the business to achieve?

- To continue making calls using the Telstra-held Australian Caller IDs that you have as Caller IDs with Twilio, port your Phone Numbers from Telstra to Twilio. Porting Phone Numbers usually takes 4-6 weeks.
- To use a Twilio Outgoing/Verified Caller ID to enable a call back from users, you can use a Twilio Phone Number for making outbound calls and then use call-forwarding for receiving inbound calls, by following these steps:
  - Submit the information outlined in Regulatory Requirements for Australia to get a new Twilio Phone Number. Please follow the process outlined here for submitting the required regulatory information through the Twilio Console for approval.
  - Once the regulatory information is approved, you can get a new Phone Number via the Twilio Console or the Twilio API. It will take 2-3 weeks to receive the new Phone Number.
  - To redirect your inbound calls to your desired Phone Number, you can enable call forwarding on your new Twilio Phone Number.

What will non-compliance cost our business?

If you make calls to Australian Phone Numbers on the Twilio network, using phone numbers not assigned to you by Twilio, the calls might be blocked by Australian operators.

How can contactSPACE solutions assist with this requirement?

- Please get in touch with contactSPACE to get access to suitable SIP trunking that is supported on your Twilio platform.

The Spam Act

What is it?

The Spam Act of 2003 is a piece of Australian legislation regulating the transmission of email and other electronic messages.

The key points of the act provide that:

- Unsolicited commercial electronic messages must not be sent unless it is a designated commercial electronic message defined at Schedule 1 of the act.
- Commercial electronic messages must include information about the individual or organization who authorized the sending of the message.
- Commercial electronic messages must contain a functional unsubscribe facility.
- Address harvesting software must not be supplied, acquired, or used.
- An electronic address list produced using address harvesting software must not be supplied, acquired, or used.

It is also against the spam rules to:

- Help, guide or work with another person to break the spam rules.
- Encourage another person to break the spam rules.
- Be directly or indirectly, knowingly concerned with breaking the spam rules.

What businesses does this apply to?

- All Australian businesses that send electronic messaging, including telephone calls to Australian residents.
- All businesses operating in Australia that store, disseminate or disclose personally identifiable data.
- Businesses seeking to adopt industry best practice per Australian legislation.

The Crown (The Commonwealth Government) is exempt from the Act.

Mandatory?

Yes.

What regions does this apply to?

Australia.

Use of contact-tracing information

If your business is keeping customer records for contact-tracing, any phone numbers and email addresses you acquire for this reason cannot be used for marketing. You may face serious penalties for misusing this information.

What does it cost the business to achieve?

Achievement of Spam Act compliance may be undertaken be in conjunction with other compliance certification endeavors that your business may be undertaking, like ISO 27001 or compliance with the Privacy Act.

For an organization with no other compliance in place, looking to begin the steps to operate in a compliant manner, the following aspects could be taken into consideration:

The Spam Act (Cont.)

Component	Cost	Time
Spam Act regulatory Assessment	$20,000 – $30,000	2 weeks full time internal team
Complete Spam act audit	$20,000 – $50,000	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

What will non-compliance cost our business?

The Act details specific penalties allowable under law. Maximum penalties for repeated violations extend to AUD$2.2 million for each day the violations occurred.

The main remedies for breaches of this Act are civil penalties and injunctions.

In 2020-2021:

- Woolworths Group was fined AUD$1,003,800.
- Optus (Singtel) was fined AUD$504,000.
- Kogan was fined $310,800.
- Telco First Pty Ltd was fined $79,800.
- It was reported that $2,194,500 in penalties were issued in the last two years.
- ACMA conducted 29 investigations into telemarketing spam.

In addition to financial penalties, ACMA has the capability to:

- Issue formal warnings.
- Issue infringement notices.
- Seek civil penalty from the Federal Court.
- Seek court enforceable undertakings.

The Spam Act is enforced by the Australian Communications and Media Authority (ACMA).

ACMA advise that businesses are on notice that they must have compliant unsubscribe systems and practices in place. The penalties for breaching can be financially serious and reputationally damaging.

In the opinion of the court when addressing spam, *"The spam rules have been in place for seventeen years… the scale and prolonged nature of the non-compliance is inexcusable."*

How can contactSPACE solutions assist with this requirement?

We are specialists in multiple contact center verticals requiring varying levels of Spam Act compliance, such as the financial services industry, service industries, fundraising, education, and healthcare.

Using contactSPACE, you can ensure that:

- You give people an easy way to unsubscribe, whether you're reaching them over the phone, via email, or using SMS.
- Your agents clearly state who they are calling from, using contactSPACE CallGuides. You can also automate compliance assurance using contactSPACE speech analytics.

The Privacy Act

What is it?

The Privacy Act of 1988 is the principal piece of Australian legislation protecting the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information in the federal public sector, as well as in the private sector.

The Privacy Act is broad legislation. It addresses areas of concern including privacy regulations, credit reporting, health, and medical privacy. It even addresses the privacy of an individual who has been listed as missing.

What businesses does this apply to?

- All Australian businesses that make and receive telephone calls while subject to compliance and privacy regulations.
- All businesses operating in Australia that store, disseminate, or disclose personally identifiable data.
- Businesses seeking to adopt industry best practice per Australian legislation.

Mandatory?

Yes.

What regions does this apply to?

Australia.

What does it cost the business to achieve?

Achievement of Privacy Act compliance will likely be undertaken in conjunction with other compliance certification endeavors, such as ISO 27001 or compliance with the Spam Act. These endeavors will typically overlap to the Privacy Act legislation and will mitigate duplication of compliance efforts.

For an organization with no other compliance in place, looking to begin the steps to operate in a compliant manner, the following aspects could be taken into consideration:

Component	Cost	Time
Privacy Act regulatory assessment	$20,000 – $30,000	2 weeks full time internal team
Complete Privacy Act audit	$20,000 – $50,000	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build Vs buy decisions	$5k – $50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

The Privacy Act (Cont.)

What will non-compliance cost our business?

Maximum fines for breaches of the Privacy Act are AUD$420,000.

Further, businesses that have breached the Act have also been ordered by the Privacy Commissioner to:

- Issue an apology.
- Adopt and implement remedial measures in response to privacy breaches.
- Review their privacy/information handling policies and procedures, conduct staff training, and make necessary changes to ensure information is accurate, complete and up to date.
- Undertake an independent audit of their policies and operation processes.
- Review new remedial measures adopted and reports the findings of that review to the OAIC.
- Reimburse reasonably incurred costs and expenses.

How can contactSPACE solutions assist with this requirement?

We are specialists in multiple contact center verticals requiring varying levels of compliance, such as the financial services industry, service industries, fundraising, education, and healthcare.

Our solutions have been built with compliance to the Privacy Act in mind. To that end, we are more than happy to address any vendor questions that may arise from topics such as:

- Data management
- Encryption
- Baseline security controls
- IAM and people management
- Cybersecurity
- Fourth party risk
- Cloud risk assessments

> Our solutions have been built with compliance to the Privacy Act in mind.

SOC 2 Certification

What is it?

SOC 2 stands for System and Organization Controls.

Specifically, it is the name of a suite of reports produced during an audit. The controls are a series of standards designed to help measure how well a service organization conducts and regulates its information.

SOC 2 reports also analyse other elements of the business, such as availability, payment processing security, administration security, privacy, and confidentiality.

Becoming SOC 2 compliant shows that you are willing to take the time and make the financial investment to ensure that your client data is secure. A clean SOC 2 report is like a badge of honour that you can show to others who want to work with or invest in your business.

SOC 2 is broken down into two parts:

- SOC Type 1 is where your organization receives a legally binding agreement called an SOC 2 report. The report lays out the design of the security process is that will operate at a specified date. It also includes the planning behind existing policies, internal controls, and operating procedures.
- SOC Type 2 is where your organization receives ongoing reports on how effective these controls are over a specific period. The usual period is 9-12 months.

What businesses may benefit from achieving this certification?

- Service organizations.
- Travel industry.
- Organizations that wish to obtain competitive advantage.
- Organizations seeking structure on the design of internal controls.
- A business seeking peace of mind.
- Any organization seeking regulatory compliance – SOC 2 audits dovetail into other regulatory frameworks like HIPAA and ISO 27001.

Organizations that do not host financial data may find that that this is the only compliance auditing that is required. On the other hand, organizations that do host financial data may require other certifications in addition to SOC 2.

Mandatory?

No.

What regions does this apply to?

Global.

What does it cost the business to achieve?

A combined fee for first time Type 1 and Type 2 reports would typically be in the range of $50k-$150k. This also considers lost productivity, build vs buy decisions for new tools, and security training.

The cost of an auditor for SOC 2 Type 1 audit may be in the $12k-$17k range.

Component	Cost	Time
Readiness assessment	Productivity loss of dedicated team	2 weeks full time internal team
Legal	$10,000	2 weeks spread out over 3 months
Build vs buy decisions	$5k-$50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

SOC 2 Certification (Cont.)

What will non-compliance cost our business?

SOC 2 compliance is not a mandatory certification. It is however considered a form of best practice in operating a business and provides the framework for incorporating multiple compliance factors and responsibilities in a single audit result.

The risk to the business to not have a defined and agreed upon series of organizational standards can be immense:

- Loss of competitive advantage and revenue.
- Inefficiencies in internal controls.
- Lack of compliance and the ability to conduct suitable auditing.
- Exposure of the business to risk, including litigation.

How can contactSPACE solutions assist with this requirement?

- We help to relieve some of the SOC 2 compliance burden, especially as it pertains to your contact center information technology, through the security of our application.
- Our system is built on the principles set out in ISO 27001, laying the security foundations for achieving SOC 2 compliance.
- For example, data processed in contactSPACE is encrypted at rest and in storage, ensuring complete data security.

AICPA SOC

SOC 2 TYPE II

CERTIFIED

Payment Card Industry Data Security Standard

What is it?

Payment Card Industry Data Security Standard (PCI-DSS).

The purpose of PCI-DSS standardization is to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data.

PCI-DSS is a standard that has been prescribed by the Payment Card Industry Services Council, originally formed by American Express, Visa, Mastercard, Discover and JCB International.

The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called “control objectives”. The six groups are:

1. Build and Maintain a Secure Network and Systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

PCI DSS Onsite Assessments determine the data security posture of your organization.

All companies who are subject to PCI DSS standards must be PCI compliant. There are four levels of PCI Compliance, and these are based on how much money you process per year, as well as other details about the level of risk assessed by payment brands.

At a high level, the levels are:

Level 1 – Over 6 million transactions annually

Level 2 – Between 1 and 6 million transactions annually

Level 3 – Between 20,000 and 1 million transactions annually

Level 4 – Less than 20,000 transactions annually

What businesses does this apply to?

- Any organization that handles or processes branded credit cards from a major card provider scheme.
- Businesses that must demonstrate compliance with all PCI DSS requirements annually.

Mandatory?

Yes. For organizations that meet the above criteria. The mandatory specifications ensure continued capability to offer credit card processing.

What regions does this apply to?

Global.

Payment Card Industry Data Security Standard (Cont.)

What does it cost the business to achieve?

Whilst not an exhaustive list, components to consider to achieve PCI compliance include:

Component	Cost	Time
PCI-DSS gap analysis	$20,000- $30,000	2 weeks full time internal team
Complete onsite assessment	$20,000-$50,000	2 weeks full time internal team
Remediation and retesting	$10,000	Up to 6 weeks
Legal	$10,000	2 weeks spread out over 3 months
Report on Compliance (ROC) submission and certification	$10,000	
Build vs buy decisions	$5k-$50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

What will non-compliance cost our business?

If your PCI validation is delayed, you could lose time, money, and other valuable resources.

Failure to obtain or complete certification may result in an organization's ability to provide financial payment processing being revoked by the payment gateway provider. This exposes the business to significant financial loss.

Also, a failure to maintain PCI compliance can pose a significant risk to your brand. If customer card details are exposed, this can have a massive impact on your business's reputation, even if your ability to process payments remains unaffected.

How can contactSPACE solutions assist with this requirement?

contactSPACE was an early adopter of the Payment Card Industry Standard, and currently helps many contact centers process PCI compliant payments both in-conversation with an agent, and automatically using IVR.

pcipayspace is our innovative payment processing solution, which allows you to take automated IVR payments, or have your agent guide customers through the transaction – inputting card details using their phone keypad in a PCI complaint manner. It enables you to get on with what's important – taking payments efficiently, maximizing your conversion rates, and minimizing IVR abandonment.

ISO 27K

What is it?

ISO27K is the family of information security standards published by the International Organization for Standards.

The ISO controls that are relevant to contact centers include:

- 27001: An international standard on how to manage information security. It details the requirements for establishing, implementing, maintaining, and improving an information security management system (ISMS).
- 27002: An international best practice recommendation for personnel responsible for initiating, implementing, or maintaining an ISMS.
- 27005: Provides guidelines for the establishment of an ISMS as per the concepts specified in ISO 27001.

What businesses does this apply to?

All.

Mandatory?

No. Whilst not mandatory, ISO 27001 has certainly been accepted as a global best practice on the subject of information security documentation and planning.

What regions does this apply to?

Global.

What does it cost the business to achieve?

Component	Cost	Time
Precertification Phase I: (e.g., scope definition, risk assessment, risk treatment plan, gap assessment, phase II remediation plan)	$20,000- $30,000	2 weeks full time internal team
Precertification Phase II: (e.g., gap closure (collaboratively), registrar selection, ISMS Artifact development, Risk Management Committee, Incident Response, Internal ISMS Audit, On-site Certification Audit Support)	$20,000-$50,000	2 weeks full time internal team
Certification audit	$10,000	Up to 6 weeks
Surveillance auditing	$7,500	2 weeks spread out over 3 months
Internal compliance auditing	$7,000	Ongoing
Report on compliance (ROC) submission and certification	Up to $3,250	
Build vs buy decisions	$5k-$50k depending on mix of commercial and DIY	2 months
Staff training	$5,000	1 week
Auditor	$17,000	1 month
Project lead	$75,000	6 months
Tools	$30,000	N/A

ISO 27K (Cont.)

What will non-compliance cost our business?

- Loss of competitive advantage and consumer confidence.
- A risk that, in not following best practice standards, the business may be exposed to security risks and fines at a future date.

How can contactSPACE solutions assist with this requirement?

Our team has a wealth of experience with the ISO 27K suite of standards. contactSPACE would be pleased to work with your organization on responding to questions contained in a Standardized Information Gathering (SIG) questionnaire.

Our solutions have been built with regulatory compliance in mind, particularly information security. To that end, we are more than happy to address any vendor questions that may arise from topics such as:

- Data management
- Encryption
- Baseline security controls
- IAM and people management
- Cybersecurity
- Fourth party risk
- Cloud risk assessments

> Our solutions have been built with regulatory compliance in mind, particularly information security.

SIG

What is it?

Standardized Information Gathering.

SIG is a questionnaire framework that assesses risk areas including cybersecurity, IT, privacy, data security and business resiliency. The questionnaire framework is maintained by a non-profit, Shared Assessments.

SIG incorporates many industry standards, such as TCPA, GDPR, HIPAA and ISO 2700.

SIG enables a business to conduct their own questionnaires, with questions from an available repository of around 1200 questions.

What businesses does this apply to?

- Businesses engaging with a third-party supplier may choose to use these questions to run an initial assessment.
- Businesses engaging with a third-party contractor may choose to use these questions as part of their information gathering risk assessment.

Mandatory?

No.

What regions does this apply to?

Global.

What will non-compliance cost our business?

Failure to verify a contractor or vendor's qualifications may expose the business to unnecessary risk, including risk of non-compliance with dialing legislation.

SIG goes a long way toward delivering required questions in an industry standard fashion. SIG has been accepted as a method of best practice when a business is undertaking the appointment of a contractor or supplier.

How can contactSPACE solutions assist with this requirement?

Many contactSPACE customers choose to rely on the SIG process to obtain their pool of questions when conducting vendor assessments. We are familiar with this process.

contactSPACE would be pleased to work with your organization on responding to questions contained in a SIG questionnaire.

Our solutions have been built with compliance to regulations in mind, particularly information security. To that end, we are more than happy to address any vendor questions that may arise from topics such as:

- Data management
- Encryption
- Baseline security controls
- IAM and people management
- Cybersecurity
- Fourth party risk
- Cloud risk assessments

What does it cost the business to achieve?

Component	Cost	Time
SIG single license from Shared Assessments	$10,000	2 weeks full time internal team
Third Party Risk Toolkit license from Shared Assessments	$15,000	2 weeks full time internal team
Questionnaire preparation by team	$2,500	Up to 1 weeks

Data Isolation & Single Tenant Architectures

What is it?

When storing information in a cloud environment or data center, in a single-tenancy architecture every tenant will have their own single database and software instance. In a multi-tenanted solution, multiple tenants share the same architecture, like servers, or the same software, as in a phone system or contact center technology.

What businesses does this apply to?

- Any business consuming a cloud service from a third-party vendor.
- Any business considering storing their information on shared architecture.

Mandatory?

No.

What regions does this apply to?

Global.

What does it cost the business to achieve?

A multi tenanted solution may come with lower initial set up and ongoing costs. Because the tenancy is shared, often a vendor will only maintain the software on a multi tenanted solution at the same release. This means that your business may be forced to be reactive within your vendor's patching and upgrade schedule.

The slightly larger up front and ongoing costs arise from the fact that the cloud provider must provide a single instance of its architecture for your business's sole use. With a single tenanted solution, storage and consumption fees apply to the vendor for that individual instance, the costs of which are difficult to balance out over multiple customers at scale.

A multi-tenant solution cannot provide the same level of security controls that may be available to a single tenant solution. This is because those same security controls apply to other tenants on the same architecture.

What will non-compliance cost our business?

Failure to comply with relevant legislation such as GDPR and HIPAA may expose your business unnecessarily to risk, including the risk of fines from regulators.

Each tenant's data should also have an isolated backup, so if there is any data loss, tenants should have an easy time restoring their data. When data space and servers are shared in a multi-tenant environment, a service provider may only restore their base backups to your solution. Unnecessary data loss, privacy breaches and more may arise in the event of a system failure.

A multi-tenanted solution increases the risks that are inherent in delivering an updated version of software. It increases complexity of design and adds to professional workload to change the system. Software updates in a multi-tenanted solution are rolled out to all tenancies simultaneously, regardless of how it impacts your business.

How can contactSPACE solutions assist with this requirement?

contactSPACE utilizes single tenant architectures built with data isolation, security and compliance with legislation in mind.

Our architecture is built around a multi-instance cloud solution, where each client is segregated into their own logical environment. There are many advantages to this configuration, including improved performance, stability, security, flexibility, and reduced costs.

Using Skills for Compliance

What is it?

Skills in a contact center are used to categorize and qualify agents and their work types.

Skills may be given priorities, or rankings, against which an agent or work item can be ranked.

For example, an inbound agent who is highly trained in customer contracts may be given a skill of ''contracts 10''. When a call with a skill requirement of a level 10 contract agent is received, the call will be routed to the most qualified agent who is available.

Outbound agents can also be prevented from dialing records which they are not appropriately skilled or qualified to contact. Data can be assigned with minimum skill level requirements before an agent is permitted to interact with that particular record.

Providing access to records on which an agent is not trained to handle may create a violation of one or more of the regulations described in this document.

What businesses does this apply to?

- All businesses that make and receive telephone calls while subject to compliance and privacy regulations.
- Businesses seeking to adopt industry best practice.

Mandatory?

No.

What regions does this apply to?

Global.

What does it cost the business to achieve?

Skills-based routing is available as a function of your contact center software solution. Businesses using contactSPACE can use skills-based routing at no additional cost. Some administrator time will be required to set up and test skills-based routing logic.

What will non-compliance cost our business?

Agents who are not skilled or trained on an area of business should not be permitted to work on tasks that carry skilled requirements. Otherwise, the business may find itself in breach of data privacy regulation, and it may also fail to comply with certified best practice, such as ISO 27001.

How can contactSPACE solutions assist with this requirement?

Skills based routing is available to all contactSPACE customers. It is the cornerstone of effective agent assignments and enables you to triage work very effectively for your contact center, based on the skill and training of the agent.

Using contactSPACE skills-based routing, you can either assign work to specific agents, or teams of agents. It may be that you have team members with specific skillsets, or have groups of agents with the right training, qualifications, and/or licensing for specific pieces of work. In this case, you can easily create skills groups, avoiding the need to keep track of skills assigned to hundreds or thousands of individual agents.

Conclusion

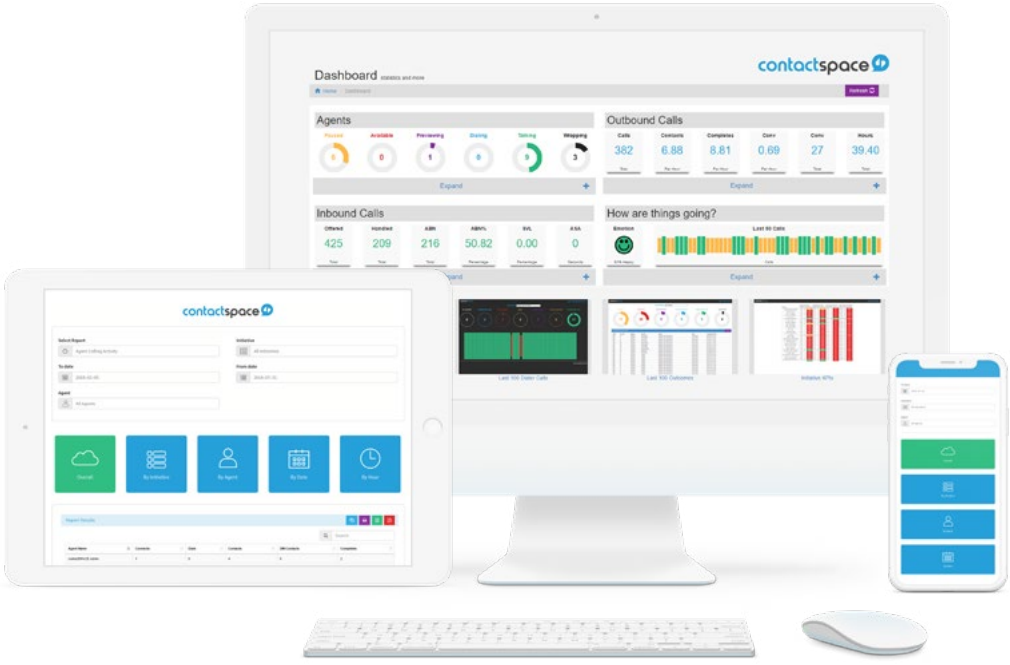
Ensuring your contact center remains compliant with all applicable rules and regulations may seem a difficult task. There are currently so many different pieces of legislation that the cost of compliance can seem eye-watering.

However, with the right software solution in place, this can significantly reduce the amount of work you have to do to ensure compliance.

For example, with contactSPACE, our system architecture and security protocols help you to achieve many of the requirements necessary for compliance with security and privacy legislation. Plus, contactSPACE makes it easy to ensure outbound dialing compliance, no matter the specific rules that apply in each region you make calls.

To learn more about contactSPACE, and to see if we can help you achieve your compliance goals, get in touch with us at:

info@contactspace.com



Thank you.

Level 9, 1 Chandos Street
St Leonards, NSW 2065, Australia
info@contactspace.com
contactSPACE
www.contactspace.com