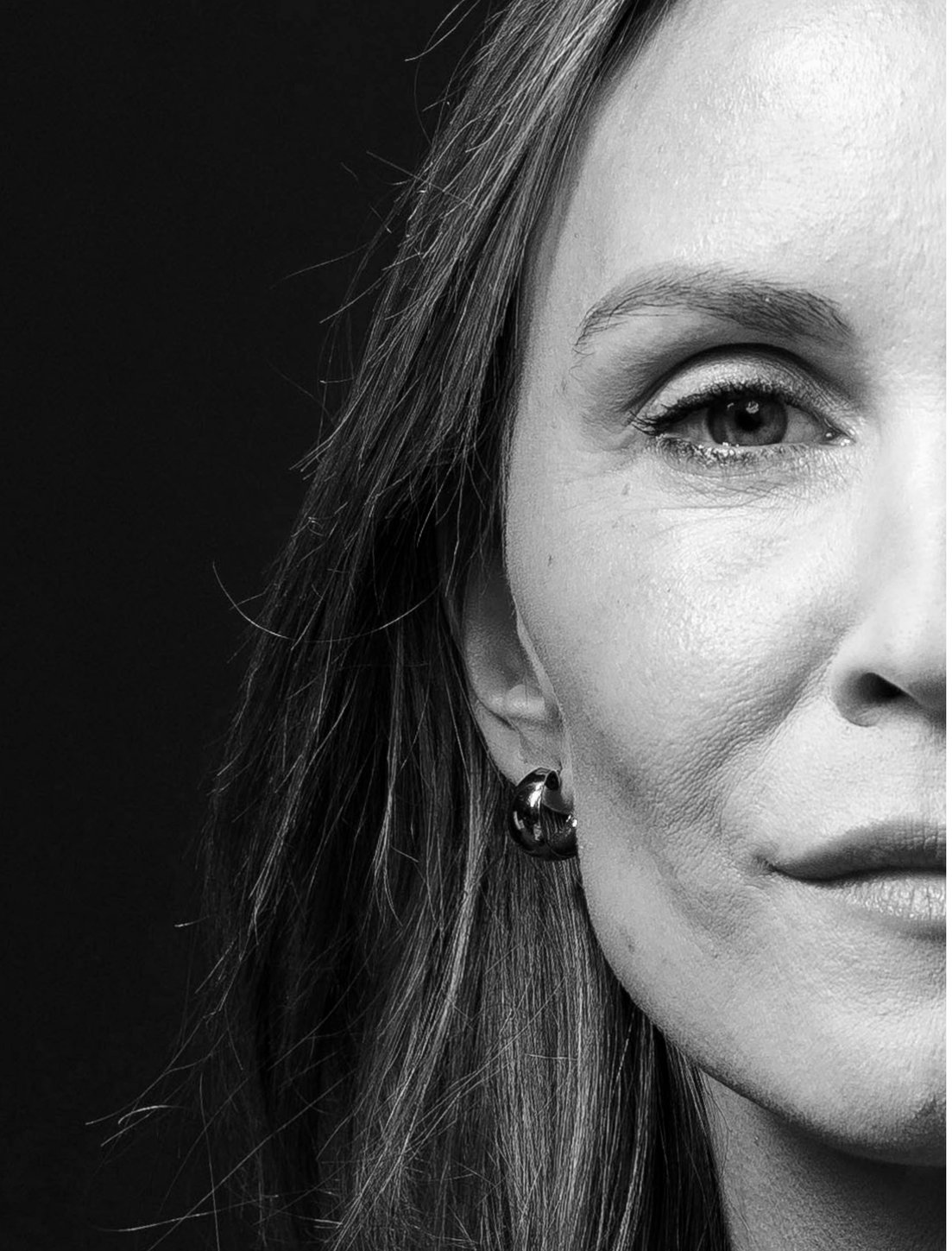


eBook

Forcepoint | Powered by ConversationalGeek

Cybersecurity, Compliance, and Protecting Critical Data

How compliance is good for an organization

A Guide to What Data Protection Regulations Mean for the Modern Enterprise and How Compliance Helps.

Regulatory compliance has never been more crucial. Countries across the world are enforcing strict rules over the handling of personal data. Sensitive corporate data, including Intellectual Property (IP) and other 'secret sauce' of a business, are at risk of cyber threats from individuals, hackers, and state-sponsored actors. In 2020, the pandemic induced a major shift to work-from-home (WFH) that added new threat vectors. An IAPP study[2] highlights employee privacy protections and virtualization challenges as the top priorities during WFH and return-to-work transitions. The IPPA study, "Building a Working World Study," also points out that privacy remains a strategic business priority. The study further highlights that policymakers, regulators, and academics were focused on "bigger-picture societal concerns" and considered the increase and normalization of surveillance by governments and commercial actors as their top priority.

But the regulatory landscape is complicated. Data protection and privacy regulations are created at local and regional levels and vary across industry verticals. Many requirements between regulations overlap, while some are highly focused, which means organizations may be affected by more than one.

This eBook will take you through a story about regulations and their impact on organizations the world over. You'll find out:

- → Why we need data protection regulations
- → The kind of data regulations protect
- → The complex nature of the modern enterprise and its data, and how risk-adaptive protection is key in securing data, ensuring privacy, and enabling business productivity
- → Why the intersection of humans and data matters
- → Important regulations, standards, and frameworks
- → Regulations across various geographies
- → How to leverage technology for compliance

"Increasingly the greatest cyber risk to your organization lies at the point of interaction between people and data, so it's clear that focusing on external threats isn't enough."

HOMAYUN YAQUB
SENIOR SECURITY STRATEGIST, FORCEPOINT[1]

[1] Forcepoint, "Balancing Data Protection and Privacy for Effectively Evaluating Security Risk"
[2] IAPP, "Building a Better Working World"

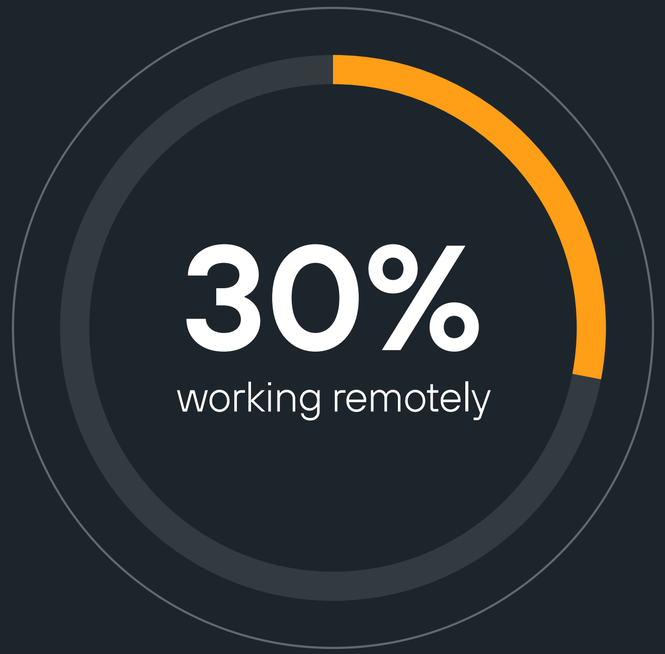
The Remote Work Era: Why We Need Regulations to Protect Data

Data protection regulations can seem at times to be barriers to business. Enormous effort, cost, and time are put in by many people to achieve compliance. Often, the hurdles needed to meet the stringent expectations of regulations can mean that an industry stumbles, deadlines are not met, and stress levels go through the roof. This situation was seen most recently with the Payment Services Directive 2 (PSD2)[3] regulation and the Strong Customer Authentication (SCA) requirement in the payments sector. The deadline for enforcing this wide-reaching regulation has been extended more than once. The European Banking Authority eventually mandated that these requirements should be fully enforced by January 1, 2021–many countries have not committed to this until later in the year.[4]

But data protection regulations are not crafted for fun. They arise in response to increasing threats against data and as a means to protect individual privacy rights. Personal data is almost becoming a currency. When something, like a digital transaction or download is free, the individual becomes the product. New threats have emerged as organizations increasingly connect across disparate sites through digital transformation programs. Cloud computing has revolutionized the way employees access apps. Smart devices and the Internet of Things (IoT) have added weight to this revolution, supporting anywhere/anytime access to data.

At the onset of the COVID-19 pandemic, many countries enforced home working. This massive shift toward WFH has added even more complex layers to the security situation. But when restrictions do eventually loosen, employees continue to work from home some or all of the time. This transition to increased remote working creates what is likely to become known as the 'remote work era.'

[3] European Commission, "Payment Services (PSD 2)"
[4] stripe.com



Through 2024, around 30% of remote employees will work permanently at home. Remote workers will represent 30% of all employees worldwide will be remote workers, or 13% growth over 2019 to nearly 600 million remote employees.

FORECAST ANALYSIS: REMOTE WORKERS FORECAST
WORLDWIDE - PUBLISHED AUGUST 21, 2020 BY ANALYSTS.
RANJIT ATWAL, ANNA GRIFFEN, RISHI PADHI, NAMRATA BANERJEE

The business data ecosystem has expanded to cover a massive series of interrelated stakeholders, from employees to non-employees, vendors, and customers. The remote work era is ultimately about an expanded critical infrastructure of data and adapting to risks. Data flows fluidly across this ecosystem. This fluidity is excellent for work and collaboration, helping productivity and business continuity. But the nature of the data lifecycle across cloud infrastructures and endpoints opens more doors for cyber criminals and allows accidental data exposure too. We are at a place where respect for privacy is key. This extends to ensuring that accidental (or deliberate) data sharing, that has not been agreed to by the data owner even with friendly organizations, is prevented.

Data is valuable to those who use it and also to those who misuse it. The value is not always monetary and depends on the type of data. Data protection regulations have to cover the widest variety of data imaginable, from personal data privacy to protecting financial data, sensitive health information, company proprietary information, and more. All of this data has intrinsic value, often beyond the price paid on the dark web.

The risks to all types of data are increasing, and regulations need to keep up with this ever-changing threat landscape. For adaptivity, data protection regulations usually start at the very beginning by reducing the issue to the data itself. Regulations define the data that they cover and then work outwards from there. But what exactly is the data the regulations are trying to protect?

One-third

By 2023, fewer than one-third of digital workers will select the corporate office as their preferred place to work

GARTNER: THE DISTRIBUTED WORKPLACE OF THE FUTURE IS NOW
PUBLISHED SEPTEMBER 17, 2020
– ANALYST SUZANNE ADNAMS

93%

93% of enterprises have a multi-cloud strategy and 59% of enterprises expect cloud usage to exceed prior plans due to COVID-19.

FLEXERA'S 2020 STATE OF THE CLOUD REPORT
» READ MORE

Here is a look at various flavors of enterprise data:

Personal Data

The use of the phrase 'personal data' is often equated with the European Union (EU) and its General Data Protection Regulation (GDPR),[5] but it is also used in several other data protection regulations as the standard definition.

With this data type, one or more pieces of information can connect to a specific individual.

Typically, data protection regulations covering personal data offer a list of attributes, including:

Name	Date of Birth
Address	Age
Email Address	Phone Number
I.P. Address	Location Data
Behavioral Data	Biometric Data
Photos	

Data breaches that expose personal information can cost organizations dearly. The UK airline, British Airways, was ultimately fined $26 million for a data breach that affected 400,000 customers. The penalty was reduced from the original $240 million, but was still the largest fine issued by the UK ICO to date. The amount reflects the impact of the loss of personal financial data, as well as the poor security measures that led to the breach.

It is also worth noting that it has taken two years between breach (2018) and fine. This may be an indicator of how long it will take before we will see fines for breaches of the U.S. California Consumer Privacy Act (CCPA).

Learn More

[5] EU Data Protection Rules

Personally Identifiable Information (PII)

This term aligns closely with U.S. regulations, and is defined by the Office of Privacy and Open Government as:

"...information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[6]

While PII is similar to 'personal data,' there is some divergence between the two. Personal data tends to have a much broader scope of data associated with an individual. However, PII can also include medical, educational, financial, and employment information. It is fair to say that much personal data is PII, but not all personal data will be covered under PII. Typically, online search data is not seen as PII as it is more difficult to link it to an individual without much effort: The key differentiator between personal data and PII being 'identifiable.'

[6] Office of Privacy and Open Government

Personal Health Information (PHI)

PHI is used as a defining character of the U.S. Health Insurance Portability and Accountability Act (HIPAA).[7]

The regulation sets out 18 identifiers under PHI:

Name	Address
Dates related to an individual (birthdate, admission date, etc.)	Telephone Numbers
Fax Number	Email Address
Social Security Number	Medical Record Number
Health Plan Beneficiary Number	Account Number
Certificate or License Number	Vehicle Identifiers and Serial Numbers, including License Plate Numbers
Device Identifiers and Serial Numbers	Web URL
I.P. Address	Finger or Voice Print
Photographic Image — Photographic images are not limited to images of the face	Any other characteristic that could uniquely identify the individual

[7] HHS.gov, "Health Information Privacy"

Financial data

Financial data can be both personal data and corporate information. Many regulations specifically focus on this type of data, such as the Gramm-Leach-Bliley Act[8] and Payment Card Industry Data Security Standard (PCI-DSS).[9]

PCI-DSS defines several types of financial data; for example, account data is cardholder data and/or sensitive authentication data.

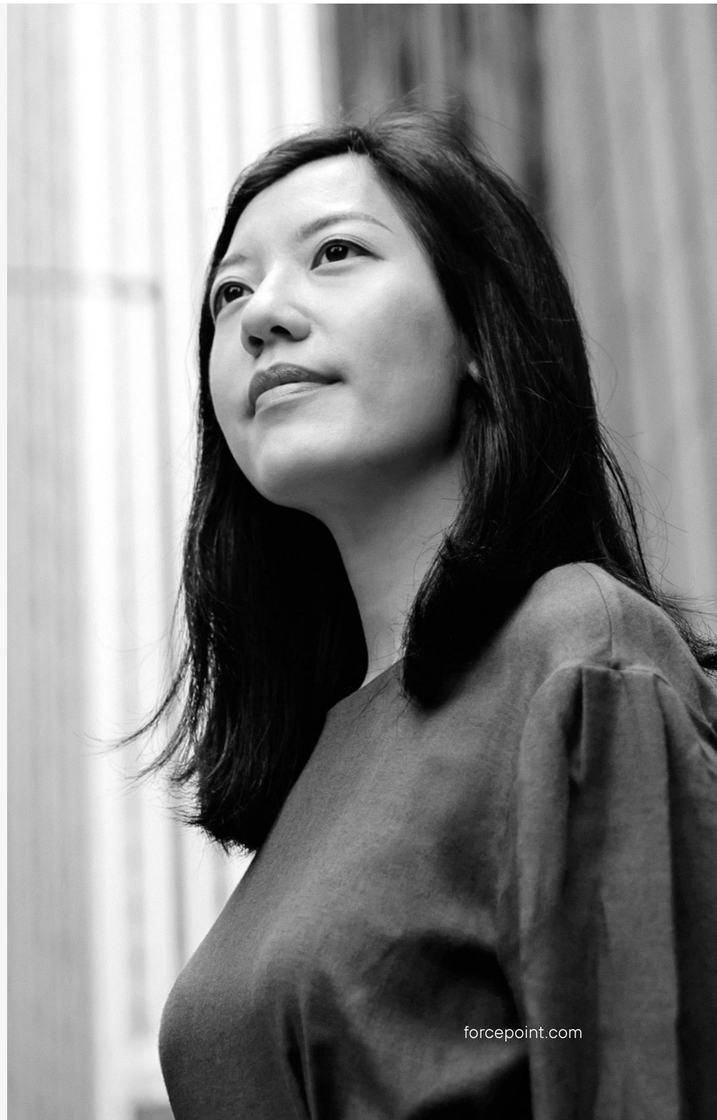
Business Identifiable Information (BII)

Data is not just personal; it can also be insider information about an organization or that which acts as the company's 'secret sauce.' The Freedom of Information Act (FOIA) defines BII as:

"...trade secrets and commercial or financial information obtained from a person and privileged or confidential." [10]

IP secret sauce is a particularly juicy steal for a cyber criminal. There are many cases of IP theft; a recent one was from chip designer AMD. The hacker posted the IP online in GitHub and boasted it was source code for new graphics hardware. AMD soon responded with its 'notice-and-takedown' process, but not before the code was in the public domain.

Learn More



[8] congress.gov
[9] pcisecuritystandards.org
[10] Freedom of Information Act

The Devil is in the Regulatory Detail

Data is the pivot upon which data regulations turn. This is obvious. However, what those regulations do to mitigate data protection risks depends on the geography, industry, and risk level. The devil is in the details, as they say, and this is borne out in practice. A PwC report, "The Adoption of Public Cloud Computing in Capital Markets," states:

> "Variations in existing regulatory requirements – such as data localization – increases the complexity for banks using the public cloud."[11]

This holds true for many industries as local and further-reaching regulations on data protection come into force.

[11] PwC, "The Adoption of Public Cloud Computing in Capital Markets"

Data protection regulations ensure that the organization's data or processes are protected against protected against increasing threats, be they malicious or accidental. Also, the appropriate use of data is an essential aspect of protecting, not just from external hackers but also from insiders and general misuse. Some data protection regulations have a large element tied to the appropriate use of data and include requirements covering the consented handling of data and its minimal collection. The latter is intrinsically linked to data protection; generally, the less data you collect, the less data you must protect, unless specific legal mandates such as retention of data are necessary.

Cyber threats and data misuse present risks across several areas:

Reputational damage

According to a Ponemon Institute study, 31% of consumers will stop using a company if a data breach happens.[12] Reputation is damaged when data is lost, stolen, exposed, or used without consent. Cyber attacks and data misuse can cost a brand its reputation, as an attack seriously impinges upon the trusted relationship between the brand and its customers. It can also result in negative comments that permeate a brand's image.

French information commissioner, CNIL, imposed a fine of €50 Million (approximately, $58 million) against Google for a GDPR violation. The fine was for general data misuse and included "lack of transparency, inadequate information and lack of valid consent regarding the ads personalization."

Learn More

Fines and sanctions

Regulations generally come with fines and sanctions to enforce adherence. Some data protection regulations carry a substantial penalty that is stringently enforced. GDPR is an example, with top-level fines of up to 4% of gross revenue or €20 million, whichever is greater.

The 2013 Yahoo data breach affecting around 3 billion accounts resulted in a massive penalty in 2018. The US Securities and Exchange Commission (SEC) issued a $35 million fine for failing to disclose the breach.[13]

Mustafa Kasim in the UK was sent to prison for six months. Kasim, an employee of Nationwide Accident Repair Services (NARS), accessed thousands of customer records containing personal data without permission, using colleagues' log-in credentials. The Information Commissioners Office (ICO) prosecuted Kasim under the Computer Misuse Act 1990 and also used regulations such as the DPA2018 to prosecute under similar charges.

Learn More

[12] Ponemon Institute study
[13] Securities and Exchange Commission

The existential threat of 'cease to trade'

If an organization turns non-compliant with specific data protection laws, including GDPR, it can face sanctions that impact trading. For example, under GDPR, Article 58 (f), a temporary or even permanent ban on data processing can be enforced. This policy would effectively prevent the business from trading.[14]

Costs

The financial damage of a data breach impacts the entire organization. Areas that incur data breach costs include remediation, brand impact, fines, and loss of business. The IBM/Ponemon Institute, "2020 Cost of Data Breach Report,"[15] offers shocking statistics, including the average cost of a data breach to be $3.86 million per breach and that 80% of breaches involve customer PII.

Share price impact

Comparitech carries out a study, updated each year, into the impact of cybersecurity attacks on company stock prices. Findings include share prices of breached companies hit a low point at 14 market days post-breach, and the fall in share price is, on average, 7.27%.[16]

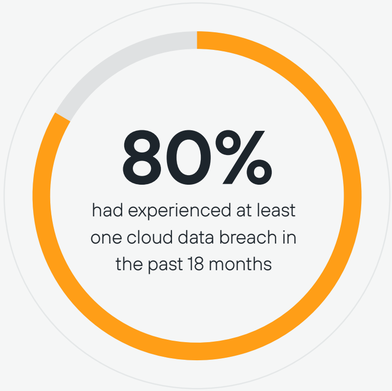
Snapchat source code was leaked when an individual looking for 'bug bounty rewards' posted code to GitHub. The individual took to Twitter to announce that he had done so in frustration at Snapchat's lack of engagement. Snapchat saw a share drop of 3.4% the day after the breach was publicized.

Learn More

Visibility cloudy

A survey by analyst firm International Data Corporation (IDC)[17] survey found that:

- → 80% of companies cannot identify excessive access to sensitive data in IaaS/PaaS environments
- → 80% had experienced at least one cloud data breach in the past 18 months
- → 43% reported 10 or more breaches



[14] DPR Article
[15] ibm.com
[16] Comparitech
[17] International Data Corporation

The Remote Work Era and What an Enterprise Is up Against

The remote work era sits squarely at the center of cyber attacks and data exposure. Data security threats come in from every possible angle. Insiders, both malicious and accidental, as well as external actors pose a risk to remotely accessed, shared, and collaborated data.

Research into this area speaks volumes:

- → **Data exposure levels:** A report from Risk Based Security into data breach levels found that between January 1, 2020 and June 30, 2020, 27 billion data records were exposed; this is over double the number exposed in all of 2019.[18]
- → **The human factor:** According to a study from Verizon,[19] 22% of data breaches included social-engineering-based attacks. Human errors also cause 17% of breaches, and 8% of breaches were due to misuse by authorized users.

  The threat isn't the corporate network. Enterprises need to think about humans the new perimeter.
- → **Remote working increases risk and cost:** The work-from-home movement during COVID-19 is increasing both the risk and cost of a data breach. According to a review by the UK government's National Cybersecurity Center (NCSC), 200 of the 723 incidents handled in 2020 related to coronavirus.[20] A survey from IBM/Ponemon found that 70% of respondents expect remote working to increase the cost of a data breach. [21]

A 2020 Malwarebytes survey found that over 55% of companies saw training home workers in data security and compliance to be the biggest challenge with remote working.

Learn More

[18] Risk Based Security report
[19] Verizon, 2020 Data Breach Intelligence Report
[20] ncsc.gov.uk
[21] ibm.com

How Is Data at Risk Today? The Human in the Machine

Data risk is, in part, about the human in the machine and how the data is used by humans. Cloud adoption has extended the enterprise footprint, and this is now further exacerbated by the remote work movement. Today, the human is the new enterprise perimeter. Cyber criminals exploit this fully by creating a complex and sophisticated web of opportunities leveraging users, entities, endpoints, and cloud infrastructures.

To further complicate matters, data protection is no longer about 'us and them.' Data misuse can even be inadvertently sanctioned by an organization when data protection regulations are misunderstood. Data misuse has many faces. Google is an example of systemic data misuse. The company was fined $57 million[22] for lack of transparency in its data use policies. The creation of secure infrastructures can help alleviate this by taking a first-principles approach. A focus on designing security systems by understanding people's intent as they interact with critical data wherever it resides is a key method of handling systemic data misuse.

To tackle the risks to data, an understanding of the fluid nature of risk and implementing dynamic policy, risk-adaptive based protection where those risks lie is fundamental:

[22] reuters.com

Phishing

The ‘evil art of phishing’ is still a favorite among cyber criminals and fraudsters. Phishing hits at the heart of the human in the machine by targeting employees and privileged users. Phishing emails are a severe threat, with spear-phishing, a highly targeted form of the technique, being most prevalent.

Verizon found that phishing remains the top attack vector, the study stating that “Phishing has been (and still remains) a fruitful method for attackers.”[23] Phishing campaigns are an indirect way to exfiltrate data by stealing privileged users’ access credentials or through malware infection.

Verizon researchers show that 22% of data breaches involve phishing.

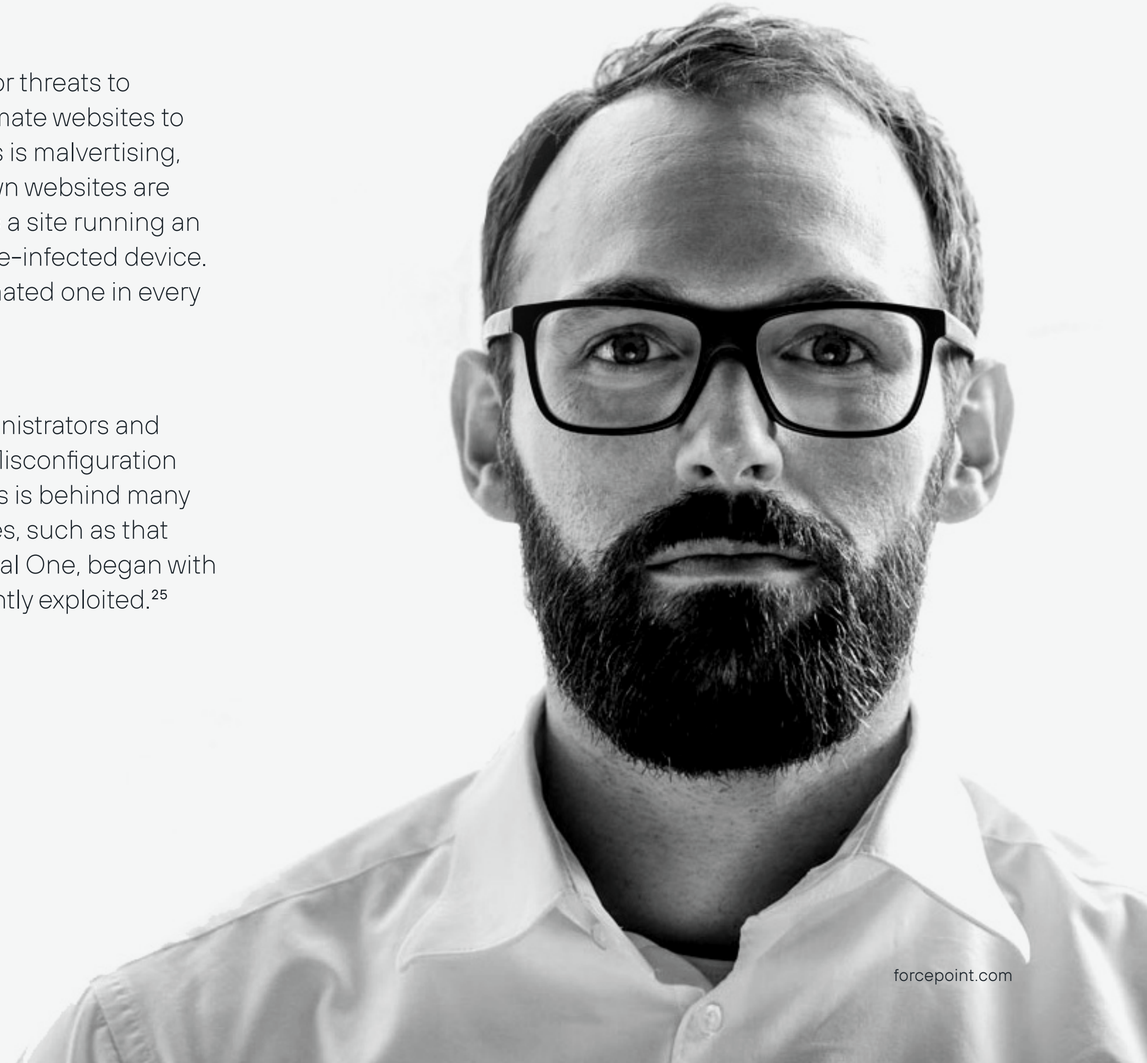
Learn More

Web-borne threats

The internet is a perfect breeding ground for threats to data. Hackers use spoof sites or even legitimate websites to carry exploits and malware. One form of this is malvertising, where (usually) legitimate ads on well-known websites are infected with malware. If a user navigates to a site running an infected ad, they may end up with a malware-infected device. Malvertising is a serious issue, and an estimated one in every 100 online ads is infected.[24]

Misconfiguration issues

To err is human. This is true for system administrators and implementation folks as much as anyone. Misconfiguration of web servers and other cloud components is behind many major data breaches. Massive data breaches, such as that affecting the 106 million customers of Capital One, began with a misconfiguration that a hacker subsequently exploited.[25]



[23] Verizon Data Breach Investigation Report 2020
[24] Media Post
[25] Krebs on Security

Lack of awareness

Just simply not being aware of the issues of data misuse and protection can result in non-compliance. Typically, the corporate workforce does not necessarily know what they are supposed to protect and, importantly, why. A lack of awareness about the security and privacy of data leads to accidental data exposure.

A lack of awareness can also lead to poorly designed data capture interfaces that ask for more data than is needed to perform a task. Data minimization policies are crucial in ensuring that designers of a UI/UX know what they should and should not collect in terms of data.

Software vulnerabilities

Malware cannot work without a little help. In addition to social engineering techniques, the malware also depends on software vulnerabilities. For example, in malvertising, infected ads use 'drive-by-download.' This effectively installs malware without the user's knowledge. Malware can only do this if the software on the user's device has a vulnerability that can be exploited to allow it to install.

Lack of knowledge of endpoints

Organizations need to know where data resides to protect it. The problem is that the modern enterprise has data that flows across multiple cloud infrastructures through extensive apps and is accessed and shared via many devices. These devices (endpoints) are a problem as they are often obfuscated from the corporate view. The lack of visibility makes it harder for an organization to apply the right security and privacy measures. Unmanaged Shadow IT devices, BYOD (Bring-Your-Own-Device), and the Internet of Things (IoT) create a cluttered landscape that blurs the universe of endpoints an enterprise knows of or has full control of.

Not applying correct security measures

Simple security measures can often be the difference between data loss and data protection. Implementing multi-factor authentication (MFA) and activity monitoring of users and entities are potent ways to control data. However, many organizations lag in using these measures.

Too many locations and point products to manage

The opposite end of the spectrum to not applying security is when an organization has too many endpoint security products. This causes issues in policy deployment and control. Non-interoperable products that do not integrate well can be as bad as poor security. Also, lack of interoperability between products can lead to inadequately shared security intelligence and interpretation.

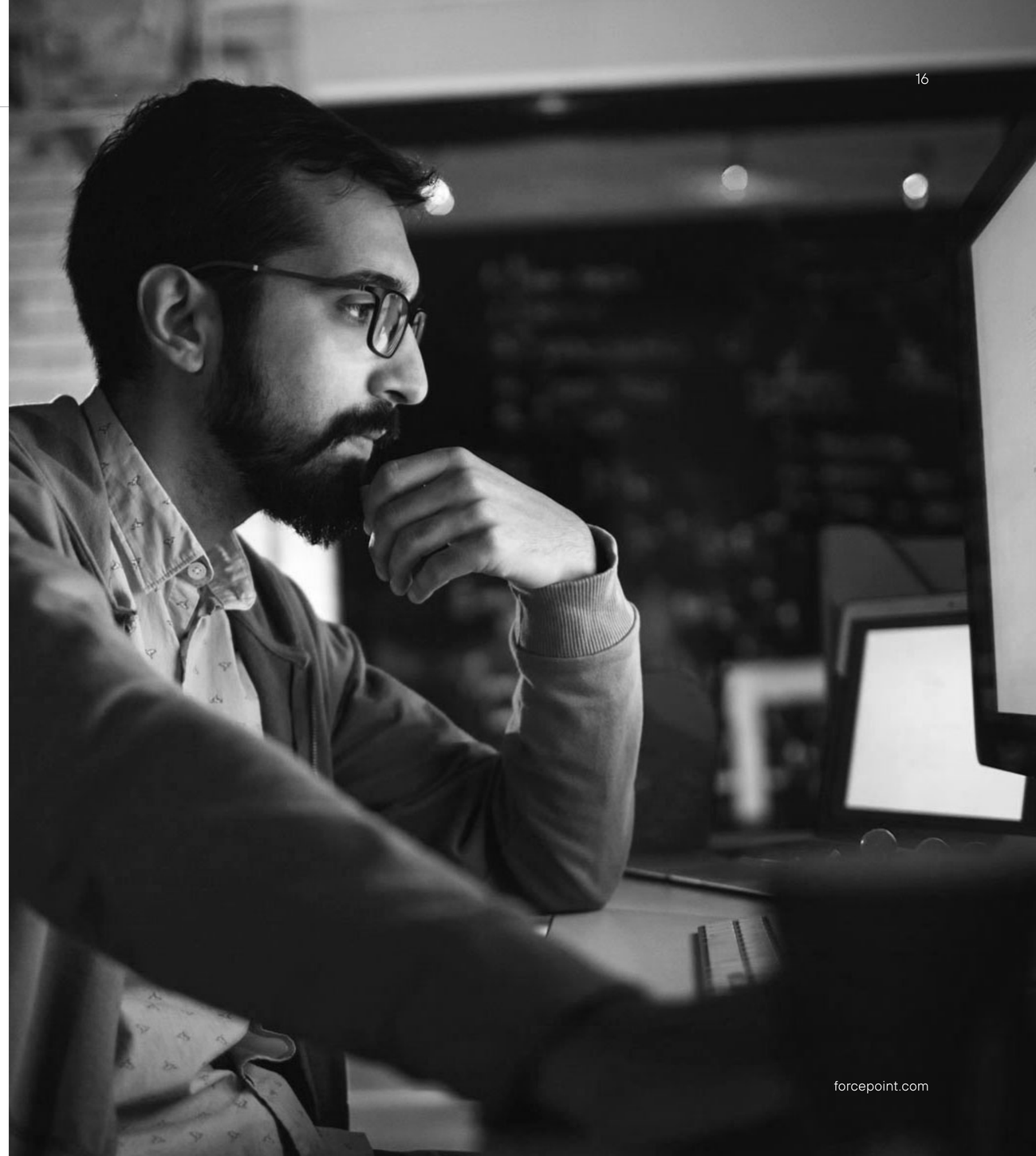
When Data Protection Gets Serious: Some Key Regulations, Standards, and Frameworks

The evolving IT environment, consumer expectations, privacy violations, and changing work patterns have prompted governments and IT industry pressure groups the world over to create and/or update regulations to stem the tide of cyber crime and data misuse.

The regulations typically reflect the technology offerings of the day. Regulations go through cycles of being updated as technology changes enter common use. As a result, regulations can become a moving goalpost and cause difficulties for firms needing to adhere to the expected measures.

Standards and frameworks are also part of the regulatory ecosystem, offering guidance and certification to prove adherence to data protection laws.

The following is a flavor of the types of regulations that span across industries and sectors.



Industry-specific and general data protection regulations – examples

→ **PCI-DSS:** PCI-DSS affects businesses that handle financial transactions. Suppose an organization accepts, stores, processes, or transmits financial card information. In that case, they must comply with PCI-DSS; this includes merchants, financial institutions (of all sizes), and payment processors (hardware and software-based), etc. The standard has six security best practice milestones that cover everything from building and securing networks to creating robust access control, monitoring, and security policies.[26]

In 2019, there were 1.7 million reports of fraud to the FTC, accounting for 53% of all reports.

Learn More

→ **HIPAA:** The U.S.-based Health Insurance Portability and Accountability Act of 1996 is specific to the healthcare industry. HIPAA is focused on the protection and privacy of health data. The data covered, of which there are 18 specific identifiers, is called Protected Health Information (PHI) and falls under the umbrella of "individually identifiable health information." HIPAA is wide-reaching, even though it is focused on healthcare. The HIPAA Security and Privacy Rules include organizations as "covered entities" required to implement the HIPAA Privacy Rule requirements. These entities, which have "business associates," must abide by stringent protection and privacy of PHI.

Healthcare is the only industry in which internal breaches are the biggest threat with 58% of incidents involving insiders.

Learn More

→ **Malicious insiders:** These are employees who misuse or abuse their access to steal, leak, or delete valuable business data out of malicious intentions. Their motivating factors are the main difference between malicious insiders and disgruntled employees. Disgruntled employees abuse data as an emotional response.

→ **Gramm-Leach-Bliley Act (GLBA):** GLBA is a U.S. federal law that focuses on financial institutions and how they communicate around customer data protection. The main rule of interest in privacy and security is the "Safeguards Rule," which is enforced by the Federal Trade Commission (FTC). The Safeguards Rule covers risk assessment. The rule states that an organization must have a written security plan based on the results of an assessment. GLBA covers many types of organizations. In a nutshell, if an organization transacts in any "significant" manner through financial products or services, that organization will need to comply.

→ **PSD 2:** PSD2 is an EU directive focusing on the end-to-end transfer of data. The regulation calls for a defense-in-depth approach. This includes two-factor authentication and network segmentation. The Secure Customer Authentication (SCA) rule has caused much upheaval in the industry. The rule, which has several caveats and derogations, requires that robust authentication is collected to secure a payment transaction.

→ **California IoT law:** This law, enacted on January 1, 2020, covers the security of IoT devices. The law describes an IoT device as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address." The law requires that reasonable security measures are applied to these devices.

[26] pcisecuritystandards.org

Standards and bodies

→ **ISO accreditation:** ISO/IEC 27701: 2019 is an expansion of ISO/IEC 27001 and ISO/IEC 27002.[27] It offers guidance on the use of Information Security Management Systems (ISMS) to include guidelines on implementing a Privacy Information Management System (PIMS). ISO/IEC 27701 defines an information classification system that provides for Personal Identifiable Information (PII). ISO 27701 also offers guidelines on implementing the standard, including Privacy Impact Assessments (PIA) and using Privacy by Design.

→ **NIST Frameworks (various):** The National Institute of Standards and Technology (NIST) provides various frameworks with guidance on data security and privacy.

These include:

- Zero Trust Architecture (ZTA): SP 800-207[28]
- Cybersecurity Framework (CSF): A guide on how to detect, prevent, and respond to cyber-threats[29]
- Privacy framework:[30] Guidance on how to identify and manage privacy risks

[27] ISO website
[28] NIST SP 800-207
[29] NIST CSF
[30] NIST Privacy Framework

The Global Take on Data Protection

Data protection is an international affair. No country is exempt from the risks of a data breach or data misuse. But each country has its way of regulating data privacy and security.

Below are some examples of data protection regulations that show how widespread the take on protecting data is. As organizations often have a global reach, these regulations can overlap, and a company may need to meet several.

→ **U.S.:** The USA uses a state-based approach to data protection law. The U.S. has a mixed bag of regulations that focus across all areas, including disposal of data, privacy, Social Security numbers, data breach notification rules, consumer data protection, and so on. The Legiscan[31] database keeps a record of U.S. legislature, including those covering data protection. There are hundreds of bills on privacy and data protection that are current. All 50 states, including the territories and the District of Columbia, have some form of data protection regulation, but none is aligned in a single federal law. At least, not as of yet, although discussions are ongoing.

An example of a US State Data Privacy Law: California's Consumer Privacy Act (CCPA)

The CCPA came into effect on January 1, 2020. The law applies to for-profit commercial Californian organizations. The CCPA defines personal data as:

"Information that identifies relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

The CCPA specifies subject rights to control data processing. Included in the act are rights to the access, portability, and deletion of data. CCPA supports the use of 'opt-out' consent in some data-processing practices. The act has stringent expectations on business accountability for data protection when collecting and handling users' personal data. CCPA fines for non-compliance are:

- $7,500 for an intentional violation of any provision, or
- $2,500 for unintentional violations

→ **EU – GDPR:** Perhaps the most infamous data protection legislation is the EU's General Data Protection Regulation (GDPR). Now in effect for over two years, the regulation has a wide-reaching impact. GDPR applies to any business, no matter where in the world it is located, if it collects, stores, shares, or processes personal data that could be used to identify an individual from an EU state.

The GDPR also classifies data, with some data being more sensitive than others. 'Sensitive' data requires higher levels of protection. The GDPR defines eight data subject rights covering the areas of data privacy of an individual. A 2020 report by the European Data Protection Supervisor (EDPS) found nearly 90% of GDPR data breaches during 2019 were a "confidentiality breach," mostly caused by human error.[32]

It is also worth noting that individual countries pass national laws that align to GDPR to comply with the regulation.

→ **UK:** The UK law that aligns to the GDPR post-Brexit is the (Data Protection Act) DPA2018. The law offers a framework for data protection in the UK The DPA 2018 moves away from the GDPR in certain areas, including having separate regimes for law enforcement authorities and the UK's three intelligence services. However, like all other countries, any UK business that handles EU citizen data will still also need to abide by the GDPR.[33]

[31] Legiscan
[32] European Data Protection Supervisor Report 2020
[33] ico.org.uk

→ **Australia:** Australia has both federal and state data protection laws. However, the Privacy Act 1988 (Privacy Act) affects any organization that handles personal data with an annual turnover of at least AU$3 million. Like GDPR, personal data (called personal information in the act) is classified into sensitive and personal data. The act sets out 13 Australian Privacy Principles (APPs), split into five key areas covering all data privacy aspects. Unlike the GDPR, the Privacy Act does not have the concept of a data controller and data processor.

Interesting fact, in Australia you must notify the authorities of a data breach within 30 days but the GDPR notification period is only 72 hours!

Learn More

→ **China:** The Cyber Security Law came into effect in 2016. The law covers network security, the protection of the rights and interests of individuals and organizations, and the secure development of technology. The Cyber Security Law expects that any organization and/or network operator that stores data within China must submit to government-conducted security checks.

→ **Brazil:** The General Data Protection Law (LGPD) was first published on August 15, 2018. This Brazilian privacy law is now expected to be enforced in August 2021. The LGPD affects all sizes of organizations, irrespective of revenue. Covered entities include those that:

- Process data within the territory of Brazil
- Offer or supply goods or services or the processing of data of individuals located in Brazil
- The personal data object of the processing have been collected in Brazil

Similar in some ways to the GDPR, the LGPD differentiates personal data and sensitive data. GDPR has eight data subject rights, but LGPD has nine. The ninth being the "right to be informed" split into two parts:[34]

1. "right to be informed of the parties the controller has shared the data with"
2. "right to be informed about the possibility of denying consent"

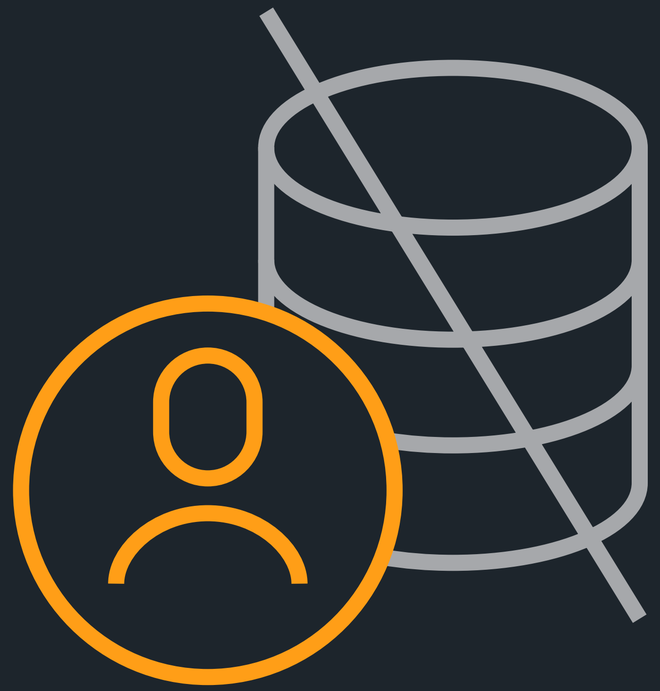
[34] iapp.org

Using Technology to Protect Data and Get Into Compliance

Data protection and privacy must be one of the most complicated areas in the technology arena.

Multiple, far-reaching, and stringent laws coupled with accidental and malicious data exposure add to an entangled problem looking for a solution. Protecting data against cyber crime and misuse is about both the process and technology, but technology shores up the process.

Here is a general look at the sorts of areas impacted by regulations and what measures are available to help protect data and prevent misuse:



Compliance in the Cloud

Securing data and systems is a holistic problem. No longer confined to on-premises security measures, data protection measures need to be both flexible and versatile. In 2020, due to the COVID-19 pandemic, almost overnight, digital transformation programs accelerated, and organizations moved onto public, private, and multi-cloud IT infrastructures and processes. These systems and business processes delivered by the cloud need to be compliant with the myriad of regulations. But how does an organization know if, by digitizing its business, it is now out of compliance? In other words, do the new appropriate levels of policy management and data protection controls previously applied map to the new infrastructure?

Cloud-delivered systems and services need to use a series of follow-up checks and regular testing to ensure that enterprise processes comply with all applicable laws and regulations. These checks, including Privacy Impact Assessments (PIA), penetration testing, and various vulnerability tests, in many cases are required, by law and to cover various directives.

Asset visibility in the cloud

The visibility of cloud-based assets is fundamental to meet regulatory compliance. These assets form the basis for data protection and privacy measures. Asset monitoring and tracking tools create asset inventories tagged with locational data. These must be classified and mapped to regulatory requirements before appropriate protection measures can be applied. Importantly, the ability to identify, classify, and track personal data, no matter where in the lifecycle, is an important feature of visibility in the cloud.

Which compliance?

Know your compliance. Regulations often focus on specific cloud-based events. For example, the GDPR specifies different protection measures if your organization is a Data Controller or Data Processor. Regular testing, such as a PIA, should be carried out against the regulatory requirements to ensure compliance.

Privacy by default and design

Cloud infrastructures and services should be implemented and configured using the principles of privacy by default and design. These principles, first developed by ex-Information and Privacy Commissioner of Ontario, Ann Cavoukian, offer guidance on delivering privacy-enhanced services.[35]

[35] IAPP, Privacy by Design

Data analytics

The use of advanced data analytics offers an insight that can afford better protection of assets. Advancements across several areas in data protection now use data analytics to provide better solutions.

Three examples of where data analytics plays an important part are:

1. Data Loss Prevention (DLP): DLP offers a set of tools used to prevent the loss of, misuse of, or unauthorized access to sensitive data. It also offers better visibility of data to add control to Personally Identifiable Information (PII) and where that PII is accessed and by whom. An organization can create pre-defined policies that apply DLP rules to various data such as business-critical, personal, customer, IP, PHI, etc. These tools help to meet regulatory compliance requirements by enforcing measures such as alerts and encryption. Good DLP should cover a wide variety of compliance across many countries. A DLP solution should locate and remediate regulated data using network, cloud, and endpoint discovery. And DLP should be able to offer central control and consistent policies across hybrid IT environments.[365]

2. Cloud Access Security Brokers (CASB): Cloud-based apps are ubiquitous across the enterprise. As remote working has added myriad endpoints, discovery and control is a vital part of any data protection posture. Gartner said,"90% of organizations that fail to control public cloud use will inappropriately share sensitive data."[37] One of the goals of a CASB is to help achieve compliance. Data protection compliance begins with the mantra "know your data." A CASB classifies this data allowing an organization to meet requirements of regulations such as the EU's GDPR. A CASB is able to automatically detect cloud application use, analyze the risks, and then enforce appropriate controls for SaaS and production applications. These controls extend to all endpoints, including personal devices used by remote workers.[38]

3. User and Entity Behavioral Analytics (UEBA): In the complicated security risk and regulatory landscape, organizations have to adapt to evolving conditions. Risk-adaptive protection offers this balance and adaptation. A UEBA platform provides deep insights into network activity to spot anomalous behaviors. Using behavioral analytics based on machine learning (ML), a baseline of interactions between individuals and data is established. This can then be used to look for unusual behavior patterns that may indicate a threat, as humans, devices, and networks interact.

UEBA tools are smart enough to determine the risk of user actions and transactions and dynamically allow low-risk events but block high-risk ones. UEBA is an essential tool in addressing regulatory requirements without disrupting day-to-day business. Evaluating when, how, and why employees interact with corporate data can help detect anomalous or abnormal behaviors that can indicate and forewarn against accidental or intentional misuse or theft of data, sabotage, or even risk to the health and safety of employees.

[36] Forcepoint DLP
[37] Gartner
[38] forcepoint.com

Automation—making compliance scalable

Many data privacy regulations come with onerous housekeeping; for example, the CCPA and GDPR stipulate the right for individuals to access their data and to see where and how it is used. This right requires managing the subjective access requests, such as, a Data Subject Access Right (DSAR) or a Subject Access Request (SAR). Robust reporting management and governance are part of mandatory compliance requirements.

These tasks quickly become laborious if not automated. Privacy rights automation is a relatively new area that can provide much-needed tools to handle data subject rights. Data clean-up can similarly be automated. If you are not legally required to retain it, processes and tools should be incorporated to remove any extraneous data. This removes the burden of management. Having a clean data policy means that redundant data does not become a liability.

Policy deployment and central management should also be part of the automation to manage the ever-evolving policies of potentially hundreds of solutions and tools.

The Office of the Comptroller of the Currency fined Morgan Stanley $60 million for failing to properly oversee the decommissioning of several data centers, putting customer data at risk of exposure. The data exposed may have included account names and numbers, Social Security number, passport number, contact information, date of birth, asset value, and holdings data.

Learn More

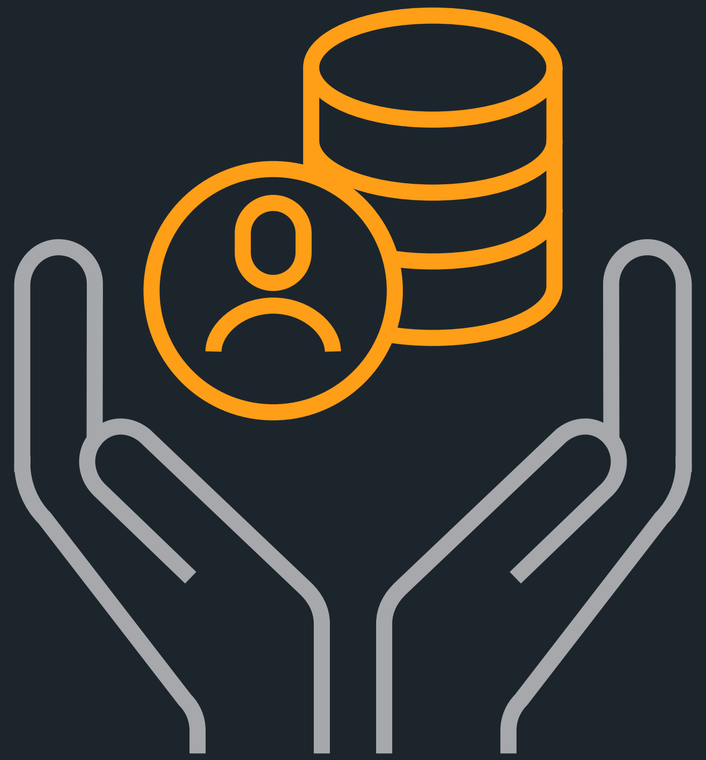
The extra mile: beyond compliance

Compliance with regulations does not necessarily imply that your data is secure. As discussed earlier, the cybersecurity threat landscape is continually evolving to take advantage of new environments and threat vectors. Handling and misuse of data is a human problem, with awareness and understanding of what constitutes misuse being a moving target.

Regulation intersects in every area involving both humans and data. Protecting critical data and intellectual property (I.P.) is crucial to maintaining a competitive and smooth-running organization.

Respect for privacy inside and out

Data protection applies to every aspect of an organization, from the new solution development to the customer experience, from UI/UX to backend systems and beyond. In protecting the rights of customers, we must also ensure we respect the privacy rights of employees. Powerful tools that contain behavioral analytics and evaluate actions must be used ethically and transparently. Security teams must work in partnership with HR and legal to ensure trust is maintained.



The Big Takeaways

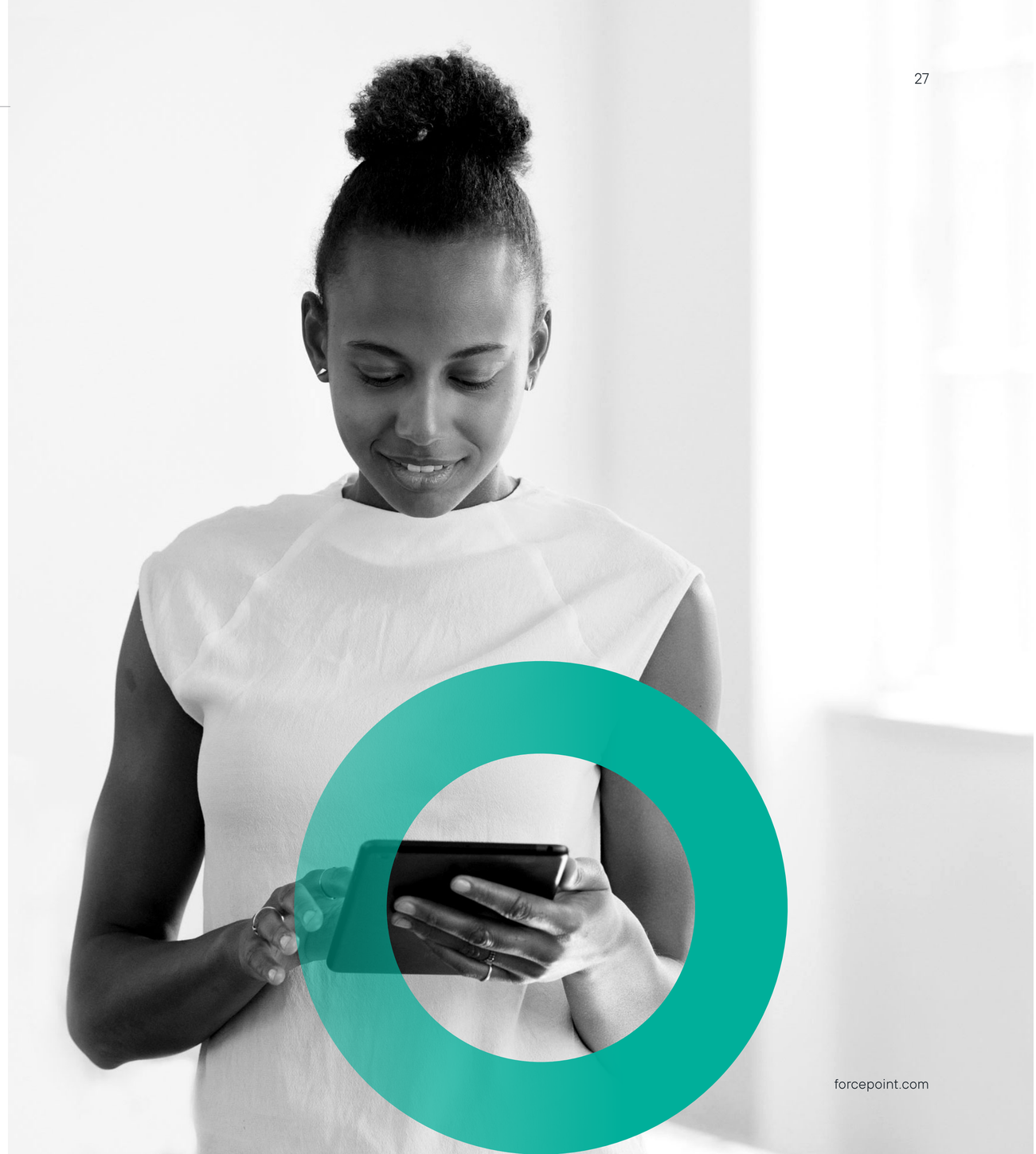
Data is a critical asset that attracts cybercrime on a massive and global scale. Personal data is indeed a commodity and of great value to the enterprise. Data is also at risk of misuse. Regulations to balance these risks provide important, often stringent, guidelines and laws on data protection and privacy.

Compliance and security should never be a roadblock to business continuity. Remaining compliant shouldn't stop users from getting work done or the business from running. Compliance and business risk are a fine balancing act. Understanding the risk levels and knowing what measures to apply to de-risk can be achieved using smart technologies and process evaluations.

The consolidation of solutions is a move in the right direction. Simplifying your compliance tools does not mean you must expect less from a solution. Automation and advanced analytics provide a modern solution to the high levels of threat under the regulatory umbrella.

Risk is not static. The solutions to de-risk should also be adaptive to the changing conditions of the modern enterprise. A process that applies risk-adaptive protection principles provides the means to apply appropriate measures based on risk. If the correct technology measures are used, they can enhance and not hinder an organization's smooth operations.

Compliance and security are not about just ticking boxes. They add real value to an enterprise. Digital transformation enforced by remote work and remote management means that compliance must adapt to the new world. By consolidating cybersecurity posture, risk-adaptive controls, and compliance requirements, the enterprise can move forward with confidence, protecting the interests and data of their customers, clients, shareholders, wider community, and itself.



Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

Cybersecurity, Compliance, and Protecting Critical Data eBook 03FEB2021