

1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context

1.4.1 Cybercrimes and data breaches



As a security professional, you are anticipated to communicate effectively with C-level executives, operational personnel, and external stakeholders such as lawyers. However, it is equally important to recognize your limitations and know when to seek legal advice when necessary.

Every organization should be addressing essential inquiries such as:

- What measures are in place to safeguard our information and assets?
- What are the information security challenges specific to our organization within a global framework?
- What is the current state of the threat landscape?

This scrutiny is crucial due to the lucrative nature of cybercrime, which often leads organizations to refrain from acknowledging victimization or pursuing cybercriminals.

While it's impossible to thwart every attack, implementing effective security measures can deter cyber intrusions by rendering them:

- Unprofitable
- Labor-intensive
- Cost-prohibitive

In essence, organizations must not present themselves as easy targets for cyber threats.




You may never achieve complete invulnerability for your company, but it's essential to find the appropriate **compromise** to ensure your company is adequately protected.

Criminals may target computers directly or exploit them to facilitate traditional criminal activities. Whether driven by profit or notoriety, malicious actors can leverage readily available tools, requiring minimal technical expertise to inflict significant damage on the digital landscape. Moreover, with nation-state actors continuously enhancing their capabilities to target information and infrastructure, today's information security professionals face an increasingly challenging task in safeguarding their environments from compromise.

The laws highlighted in the following table pertain to federal regulations in the United States. It's important to note that nearly every state in the country has implemented legislation addressing computer security matters. Due to the internet's worldwide influence, many computer-related crimes transcend state boundaries, thus falling within federal jurisdiction and undergoing prosecution in federal courts. Nonetheless, certain situations may see state laws imposing more stringent regulations and penalties compared to federal laws.

Federal Law	Description
Computer Crime and Abuse Act (CCCA) - 1984	Outlined several prohibited actions, including unauthorized access to classified or financial information in federal systems, accessing federally used computers without authorization, perpetrating fraud using federal computers (except when solely to gain computer access), causing significant damage to federal computer systems exceeding \$1,000, altering medical records in a way that affects patient care, and trafficking computer passwords with interstate commerce involvement or federal system association.
Computer Fraud and Abuse Act (CFAA) - 1986	Extended the CCCA increasing the damage threshold from \$1,000 to \$5,000 but also expanding the regulation's scope significantly. Instead of solely applying to federal computers processing sensitive data, the act now encompasses all "federal interest" computers. This broadening includes any computer exclusively used by the U.S. government or financial institutions, as well as those utilized by either entity where the offense obstructs their system use. Additionally, the CFAA extends its coverage to cases involving multiple computers used in an offense, even if they are not all situated within the same state.
CFAA Amendments - 1994	In 1994, Congress acknowledged significant shifts in computer security since the last amendment to the CFAA in 1986, leading to comprehensive revisions known as the Computer Abuse Amendments Act. These changes included prohibiting the creation of any malicious code capable of harming computer systems, expanding the CFAA's jurisdiction to encompass any computer involved in interstate commerce, permitting the imprisonment of offenders irrespective of intent, and granting victims of computer crimes the legal right to pursue civil remedies, including injunctive relief and compensation for damages.
National Information Infrastructure Protection Act - 1996	Introduced several key expansions: <ul style="list-style-type: none"> ● It extended the coverage of the CFAA to include computer systems utilized in international commerce, not just those in interstate commerce. ● It provided similar safeguards to various components of the national infrastructure beyond computing systems, encompassing railroads, gas pipelines, electric power grids, and telecommunications circuits. ● It classified any intentional or reckless actions resulting in damage to critical segments of the national infrastructure as felonies.
The Federal Information Security Management Act (FISMA) -	The National Institute of Standards and Technology (NIST), tasked with developing FISMA implementation guidelines, highlights key components of an effective information security program:

2002	<ul style="list-style-type: none"> • Conducting periodic risk assessments to evaluate potential harm from unauthorized access or modification of information systems. • Developing policies and procedures based on risk assessments to mitigate security risks and ensure security throughout the lifecycle of organizational systems. • Establishing subordinate plans for network, facility, and system security as needed. • Providing security awareness training to personnel, including contractors, to educate them on risks and responsibilities. • Performing regular testing and evaluation of security measures, with at least annual frequency. • Establishing a process for identifying and addressing deficiencies in security policies and procedures. • Implementing procedures for detecting, reporting, and responding to security incidents. • Developing plans to ensure continuity of operations for organizational information systems.
Federal Cybersecurity Laws - 2014	<p>In 2014, US President Barack Obama signed legislation to modernize federal cybersecurity efforts. This included the Federal Information Systems Modernization Act (FISMA), which centralized cybersecurity responsibility under the Department of Homeland Security, with exceptions for defense-related issues overseen by the secretary of defense and intelligence-related issues managed by the director of national intelligence. Additionally, Congress passed the Cybersecurity Enhancement Act, tasking NIST with coordinating voluntary cybersecurity standards and producing the 800 series of Special Publications. Commonly used NIST standards include SP 800-53 for federal information systems, SP 800-171 for protecting controlled unclassified information, and the NIST Cybersecurity Framework for voluntary risk-based information security. Furthermore, the National Cybersecurity Protection Act established a national cybersecurity and communications integration center within the Department of Homeland Security to facilitate collaboration between federal agencies and civilian organizations on cybersecurity risks and incidents.</p>

	<p>Scope and fines of the cybercrimes law in the table below are commensurate to the year in which they have been released.</p>
---	---

1.4.2 Licensing and Intellectual Property requirements

Intellectual property (IP) encompasses intangible assets like company names, creative works, and proprietary formulas or techniques. Laws exist to protect the rights of IP owners, ensuring fairness and preventing unauthorized use or reproduction of their creations.






With the advancement of AI, intellectual property is evolving rapidly. Be prepared to encounter related questions in your exams and address it in your cybersecurity career.





Take some time to give a look at: <https://www.copyright.gov/>

The Digital Millennium Copyright Act (DMCA) is a comprehensive United States copyright law enacted in 1998 to address copyright issues arising from the rapid growth of the internet and digital technologies. It criminalizes the production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works, as well as the act of circumventing such measures. Additionally, the DMCA provides safe harbors from liability for internet service providers and online platforms that host user-generated content, as long as they comply with certain requirements, including implementing a notice-and-takedown procedure for addressing copyright infringement claims.

The following table will show what, how and how trade secrets, patents, copyrights, and trademarks protect:

Symbol	Name	Duration	Applies to	Notes	Attacks
		<ul style="list-style-type: none"> the life of the author plus an additional 70 years for a work made for hire, the copyright endures for a term of 95 years from the year of its first publication or a term of 120 years from the year of its creation, whichever expires first 	<ul style="list-style-type: none"> Literary works Musical works Dramatic works Graphical, pictorial, sculptural work Motion pictures Sound recordings Architectural Works 	<ul style="list-style-type: none"> Guarantees the creators of “original work of authorship” protection against the unauthorized duplication of their work The creator of a work has an automatic copyright from the instant the work is created Copyright ownership always belongs to the creator of a work with the exception of works for hire (when is made for an employer during the normal course of the workday). 	Piracy: unauthorized use or reproduction of material
	Copyright				
	TM unregistered ® registered	10 years (renewable indefinitely)	<ul style="list-style-type: none"> Words Slogan Logos 	<p>Requirements to be accepted as trademark:</p> <ul style="list-style-type: none"> The trademark must not be similar another trademark. The trademark should not be descriptive of the services and goods offered (for 	<p>Counterfeiting: products intended to be mistakenly associated with brand</p> <p>Dilution: widespread use of brand name as stand-in for product (e.g. Kleenex, Xerox, etc.)</p>

					example it must not contain names).	
		Patents	20 years	<ul style="list-style-type: none"> Processes Machines Manufacture 	<p>Requirements are that the invention must be:</p> <ul style="list-style-type: none"> New Useful Not obvious 	Primarily involve infringement upon the reserved rights of the patent holder (knowingly or unknowingly)
		Trade Secrets	<p>Lifelong when protected with well stated NDAs (Non Disclosure Agreements)</p> <p>and/or NCAs (Non Compete Agreements)</p>	<p>All information that you do not want to share (best example is the recipe of Coca Cola).</p>	<p>Represent usually the best way to protect computer software, used when you need to:</p> <ul style="list-style-type: none"> Keep the information secret Keep the ownership forever <p>Everybody that is aware of a trade secret must have signed an NDA.</p>	<ul style="list-style-type: none"> Economic/industrial espionage often targets trade secrets to blunt competitive advantage or benefit from the fruit of another organization's efforts without like effort.



A patent is the strongest form of Intellectual Property Protection.

Security professionals should possess knowledge of the legal aspects concerning software licensing agreements. There are four prevalent types of license agreements in use today:

- **Contractual license agreements** involve a written contract delineating responsibilities between the software vendor and customer, commonly utilized for expensive or specialized software packages.
- **Shrink-wrap license agreements** are displayed on the exterior of software packaging and typically include a clause implying agreement upon breaking the shrink-wrap seal.
- **Click-through (or browser wrap) license agreements**, increasingly common, present contract terms either on the software box or within documentation, requiring users to actively acknowledge agreement during installation.
- **Cloud services** license agreements extend click-through agreements, often omitting written agreements and displaying legal terms on-screen for users to review, typically leading to users quickly clicking through without thorough examination.



Remember the 4 types of license agreement: Contract, Shrink-wrap, click-through, cloud services.



In a written contract, the customer typically has the opportunity to actively participate in the creation of the contract by negotiating its terms and signing the final document. However, in shrink-wrap and click-through agreements, the customer's role is limited to accepting the terms of the contract as presented by the seller or service provider. These agreements are often presented in a pre-packaged format, such as when purchasing software online (shrink-wrap) or agreeing to terms and conditions before accessing a website or app (click-through). In these cases, the customer's only option is to either accept the contract as is or decline the offer.

1.4.3 Import/export controls

The identical computers and encryption technologies utilized in powering the internet and facilitating e-commerce possess significant potential as formidable tools when wielded by a military force. Country-based rules and laws concerning import and export controls are established to regulate the movement of products, technologies, and information across borders, typically aimed at safeguarding national security, individual privacy, and economic interests.


The **Wassenaar Arrangement** aims to enhance "international security and stability" by overseeing the transfer of conventional weapons like firearms, explosives, naval weaponry, and landmines, as well as dual-use items and technologies. In 2013, the agreement underwent revisions to encompass cyber weapons, which include malicious software, command-and-control systems, and Internet surveillance tools.

The **International Traffic in Arms Regulations (ITAR)** is a US regulation designed to oversee the export of items listed in the United States Munitions List (USML), including missiles, rockets, and bombs, to maintain control over their dissemination.

The **Export Administration Regulations (EAR)** primarily addresses items intended for commercial use, such as computers and marine equipment, but also covers products with potential military applications, even if initially designed for commercial purposes.

Both the EAR and the ITAR mandate that U.S. residents seek permission before disseminating controlled technology or technical data to foreign individuals within the United States. When such information is shared with a foreign person, it is considered an export to the individual's country or countries of citizenship. To prevent a "deemed export" scenario, organizations providing information to foreign nationals must obtain a license from the U.S. government before disclosing controlled technology or technical data to nonimmigrants.

	Wassenaar Arrangement	International Traffic in Arms Regulations (ITAR)	Export Administration Regulations (EAR)
Weapons	•		•
Software/Hardware	•		
USML US Military List		•	
Commercial Use			•

	The Department of Commerce's website at www.bis.doc.gov provides a comprehensive list of countries along with their respective computer export tiers.
---	--

1.4.4 Transborder data flow

For numerous years, authorities have aimed to control the transfer of data collected within their territories to foreign nations. In certain instances, regulations aimed to safeguard individuals' private information, while in others, the state's interest lay in accessing the data for legitimate governmental needs. The advent of cloud computing and extensive data collection by public and private entities has intensified scrutiny on the transfer of such information.

The global economy thrives on data, which serves as a fundamental component of trade, generating substantial revenue even when lacking privacy-related content. Moreover, data considered legal in one jurisdiction could be deemed illegal in another, making the safeguarding of data movement a major policy priority.


Data Sovereignty is the extent to which data is subject to the laws of a country, regardless of its storage location. Data sovereignty entails the recognition that data owners or controllers must be cognizant of pertinent regulations to ensure adherence and prevent breaches of restrictions governing data usage and processing. Depending on the jurisdiction, data owners may be required to demonstrate compliance with these regulations by accounting for

their data. It's essential to understand that data sovereignty can transcend the borders of the country where the data is physically stored. For instance, data belonging to a European Union resident housed in the United States is subject to both EU and US data sovereignty regulations. It's crucial to distinguish data sovereignty from data privacy, as data privacy laws such as the European Union's General Data Protection Regulation (GDPR) prioritize responsible data safeguarding for individuals, while data sovereignty determines the scope of these data privacy laws.

Data residency pertains to where data is physically stored and processed, ensuring compliance with legal and regulatory frameworks based on its location. This concept is crucial in cloud computing and international data transfers, impacting data privacy, security, and compliance with local laws. Organizations must adhere to data residency requirements to maintain data sovereignty and protect privacy rights, as failure to comply can result in legal consequences and reputational harm.


Data localization involves storing and processing data within a specific country's borders, driven by regulatory, security, and national interest factors. It aims to exert control over data, enhance national security, ensure privacy, and support economic interests within the jurisdiction.

In summary, data residency outlines the intended geographical storage and processing of data, data sovereignty is about the rights and control over data based on the jurisdiction of the data storage and processing, and data localization mandates data to remain within a specific location and jurisdiction.

	CISOs and security professionals need to adopt a comprehensive strategy for data security. This begins by categorizing and charting the organization's data, pinpointing its storage and movement, and understanding its sensitivity, location, legal obligations, and business requirements. This analysis aids in recognizing data necessitating specific measures for residency, sovereignty, or localization, as well as third parties involved in managing the organization's data.
---	--

1.4.5 Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act)

Privacy, a longstanding principle in Western culture, dictates that information pertaining to an individual should be safeguarded from disclosure, a concept spanning millennia. However, with the advent of new technologies, this notion of privacy has been significantly challenged. Modern advancements, such as ubiquitous cellular phone tracking and detailed shopping monitoring, pose unprecedented threats to personal privacy, while governmental surveillance, including widespread facial recognition technology, further encroaches upon individual liberties. Security professionals face the formidable task of ensuring organizational activities align with pertinent privacy laws while mitigating risks associated with managing personal information across its lifecycle.

	Privacy, akin to Intellectual Property, faces significant disruption due to the pervasive influence of AI.
---	--

The following table recaps the international frameworks exist that define privacy expectations:

Framework	Description
Universal Declaration of Human Rights	Everyone is entitled to protection against arbitrary intrusion into their privacy, family life, home, or correspondence, as well as safeguarding their honor and reputation
OECD Privacy Principles	Widely adopted in international privacy laws and programs. Its eight principles cover aspects such as: <ol style="list-style-type: none"> 1. lawful and fair data collection 2. data quality 3. purpose specification 4. use limitation 5. security safeguards 6. openness 7. individual participation 8. accountability.
Asia-Pacific Economic Cooperation (APEC)	Emphasizes the protection of personally identifiable information during cross-border transfers. It highlights organizational accountability and introduces the concept of proportionality in data breach penalties

	The OECD Privacy Guidelines can be found at https://www.oecd.org/digital/privacy/
---	---

In the following we recap the most common worldwide privacy laws. These privacy laws aim to protect individuals' privacy rights, establish accountability for organizations processing personal data, and promote transparency and trust in the digital ecosystem. Compliance with these laws is crucial for businesses operating within their jurisdictions to avoid significant financial penalties and reputational damage:

General Data Protection Regulation (GDPR): The GDPR is a comprehensive data protection law enacted by the European Union (EU) to regulate the processing of personal data of individuals within the EU and European Economic Area (EEA). It imposes strict requirements on organizations handling personal data, including consent for data processing, data subject rights, data breach notification, and obligations for data controllers and processors. Non-compliance can result in severe penalties, including hefty fines of up to 4% of annual global turnover or €20 million, whichever is higher.

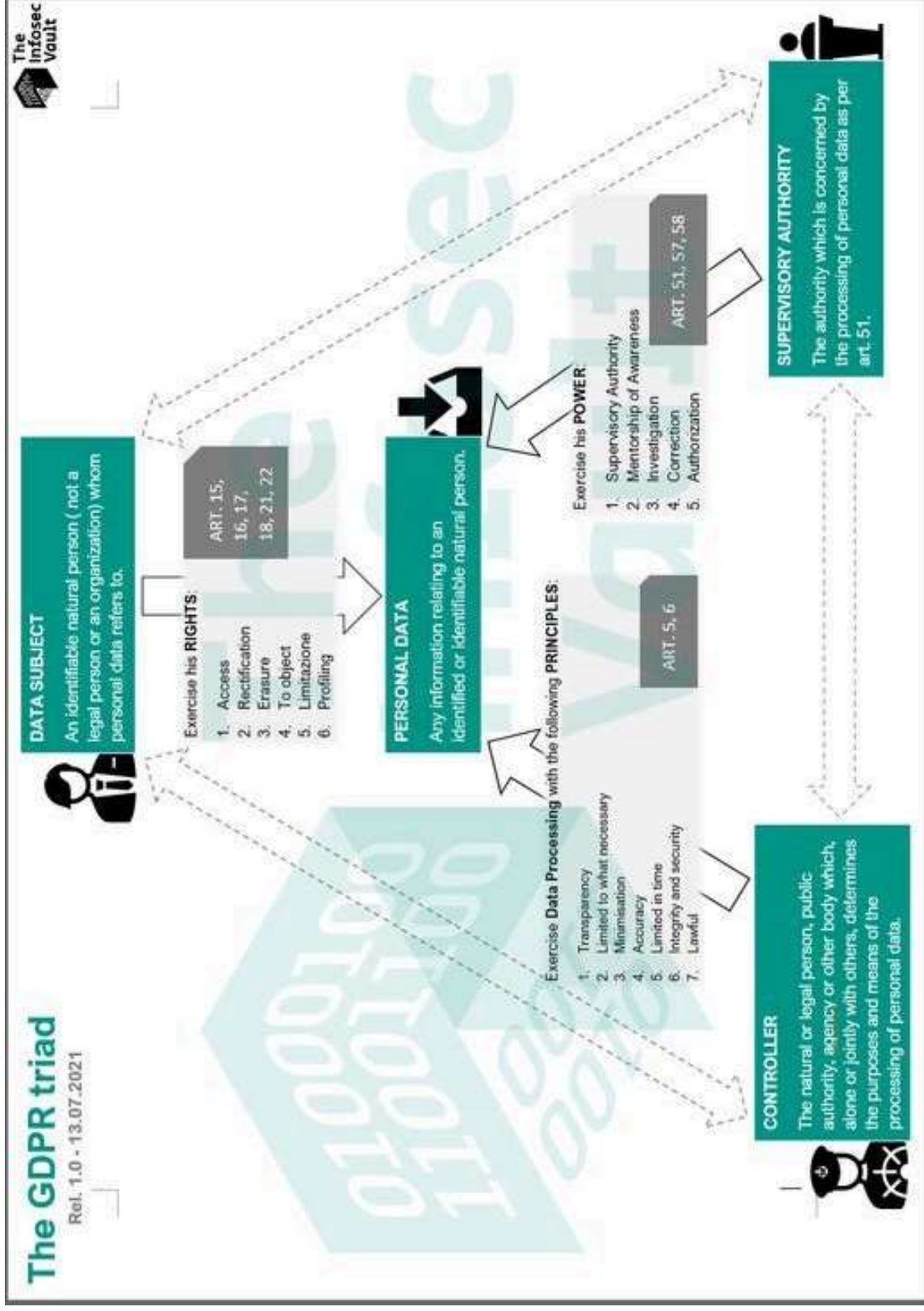
California Consumer Privacy Act (CCPA): The CCPA is a landmark privacy law in the United States that grants California residents certain rights regarding their personal

information. It requires businesses to disclose data collection and sharing practices, provide opt-out mechanisms for selling personal information, and allow consumers to access, delete, and control their data. The CCPA applies to companies meeting specific criteria, including those with annual gross revenues exceeding \$25 million or those handling large volumes of personal information.

Personal Information Protection Law (PIPL) - China: The PIPL is China's comprehensive privacy legislation aimed at regulating the processing of personal information within the country. It establishes principles for the lawful collection, use, processing, and transfer of personal data and imposes obligations on organizations to protect individuals' rights. The law introduces concepts such as explicit consent, data localization requirements, and heightened penalties for non-compliance, including fines of up to 5% of annual revenue or ¥50 million.

Protection of Personal Information Act (POPIA): The POPIA is South Africa's data protection law designed to safeguard the privacy rights of individuals and regulate the processing of personal information. It sets out conditions for lawful data processing, data subject rights, security measures, and requirements for data breaches notification. Organizations must comply with POPIA's provisions, which include hefty fines and potential imprisonment for contraventions.

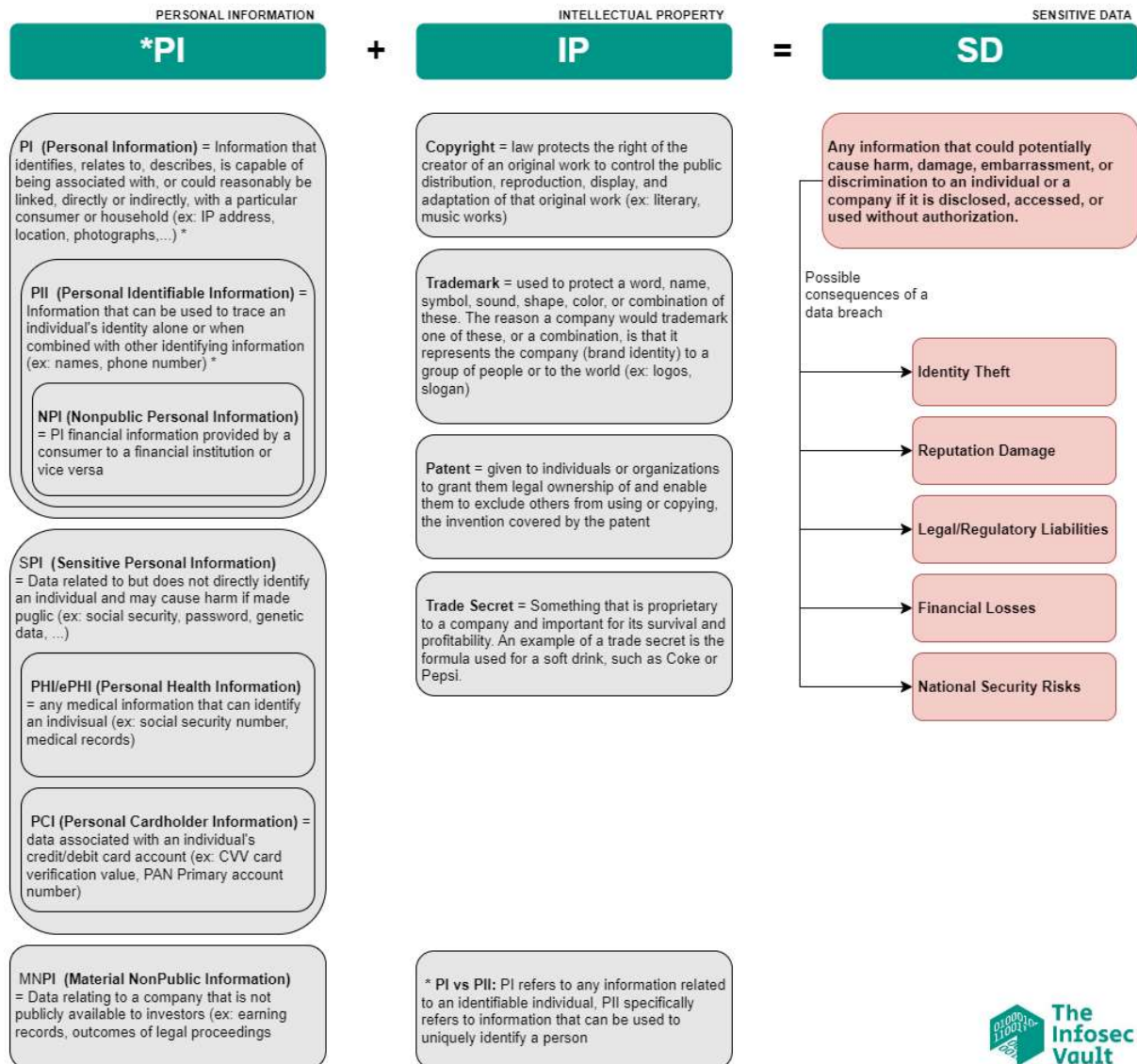
Privacy laws, including the GDPR, seek to strike a balance between the rights of data subjects, the responsibilities of data controllers, and the oversight of supervisory authorities. This equilibrium ensures that individuals have control over their personal data, organizations process it lawfully and transparently, and regulators enforce compliance to safeguard privacy rights:



The following infographic summarize the types of data we need to prioritize safeguarding within our company:

SENSITIVE DATA PROTECTION EQUATION

What data shall we take care of ?



The following table contains some common terms in use in the privacy field (many definitions are taken from GDPR and shared with other laws and regulations):

Term	Definition
Data Controller (Data Owner)	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Data Protection Officer (DPO)	An individual designated to oversee data protection and privacy matters within an organization, ensuring compliance with relevant regulations such as GDPR
Data Custodian	Need to have clearly defined responsibilities. Protect data based on the input from the owners.
Data Subject	Individual to whom personal data relates.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

A **Privacy Impact Assessment (PIA)** is a process conducted by an organization to assess whether personal data is adequately protected and to mitigate potential risks associated with it. The objectives of a PIA include identifying and evaluating privacy-related risks, determining appropriate controls to mitigate these risks, and ensuring organizational compliance with privacy regulations.

The steps involved in a PIA encompass:

1. identifying the need for the assessment
2. describing the data processing activities
3. evaluating necessity and proportionality
4. consulting relevant stakeholders
5. identifying and assessing risks
6. implementing measures to mitigate these risks
7. documenting outcomes
8. ongoing monitoring and review.



There is no need to remember the 8 standard steps of a PIA but it is mandatory to remember that a PIA is a process conducted by an organization to assess whether personal data is adequately protected.

1.4.6 Contractual, legal, industry standards, and regulatory requirements

The table below offers a basic categorization and description of contractual, legal, industry standards, and regulatory requirements (these requirements should be input for your security program):

Requirement	Description	Classification	Description
Contractual Requirements	Are obligations outlined in agreements between parties, such as service level agreements (SLAs), vendor contracts, and non-disclosure agreements (NDAs).		
Legal Requirements	Legal requirements encompass laws and regulations governing data protection, privacy, intellectual property, and cybersecurity.	Criminal Law	Encompasses regulations against offenses like homicide, assault, theft, and arson.
		Civil Law (also known as Tort Law)	Pertains to matters such as contractual disagreements, property dealings, employment issues, estate management, and probate proceedings.
		Administrative Law	Grants government bodies certain powers to establish regulations.
Industry Standards	Are guidelines and best practices established by professional organizations and bodies within specific sectors. Examples include ISO/IEC 27001 for information security management systems and NIST Cybersecurity Framework.		
Regulatory Requirements	Are mandates set forth by government agencies and regulatory bodies to ensure compliance with specific standards and protocols (examples are PCI DSS and SOX).		