

Incoming Data Protection

When it comes to data protection, enterprises often tend to focus more on the data going out. They often ignore the liability they face for the data they receive from external parties like customers, vendors, and partners.



Incoming Data Involves



Data shared for personalized services



Quotations shared by prospective vendors



Partnership agreements and NDAs sent by clients

Lack of proper protection carries risk of insider threat for incoming data

Compliance Regulations

Designed to Protect Incoming Data



The General Data Protection Regulation (GDPR)

- Intended to **unify and normalize** the **data protection framework** within the European Union (EU).
- The scope of GDPR includes all **personal data of EU citizens** processed by an organizations based inside and outside the European Union (EU).



The California Consumer Privacy Act (CCPA)

- CCPA gives Californian consumers more **rights** to the personal information they share with businesses:



Right to **know**



Right to **opt-out**



Right to **delete**



Right to **non-discrimination**



Saudi Data & AI Authority (SDAIA)

- This establishes the **legal outline for individual's rights protection personal data** by all internal and external entities of the Kingdom of Saudi Arabia (KSA). Processing personal data related to individuals residing in the KSA using any means, including online personal data processing.
- The regulation aims to achieve the following objectives related to personal data protection but not limited to:



Protect personal **data privacy** and the confidentiality of **sensitive data**.



Protect individual's right to **data privacy** when dealing with personal data and public information held by government entities.



Protect national **sovereignty**, specifically concerning personal data.



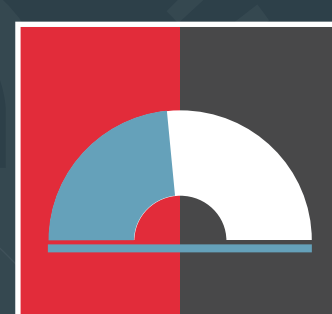
According to Gartner, Inc, **by 2023, 65%** of the world's population will have its personal data will be **covered** under modern **privacy regulations**, up from **10% in 2020**.

Stats Related to User Awareness

About Personal Data Protection



78%
Users most concerned about the security and privacy of their **financial data**



45%
Users whose **personal information** was compromised at least once in five years



64%
American Users who would hold the company responsible for the **loss of personal data**

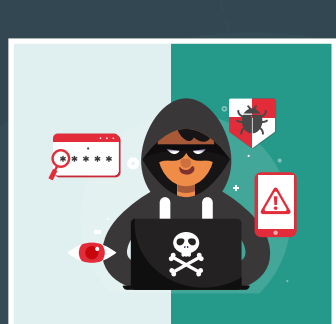


72%
UK Users who would **blame the company** and **not the hackers** for the loss of personal data

Source: <https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf>

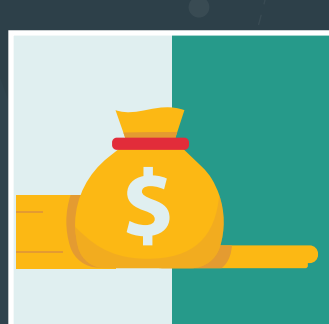
Stats Related to Breaches

Due to Not Protecting Inbound Data



780,000
Records lost
to hacking each day

Source: <https://www.upguard.com/blog/data-breach-statistics#toc-2>



137 **Records Exposed**
1.7Mn accounts breaches experienced in the **finance sector**

Source: https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_-_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

How to Protect Incoming Data?

Seclore Data Protection Portal

The external sender sends an email with attachments



Data Protection Portal tags the incoming data according to the nature of the information in it



Email protector reads the X-header and attaches usage controls to the incoming data



The internal recipient receives the information with granular usage controls and tracking

