

# Cryptographic Failures

# Protection needs of data

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS). [<sup>1</sup>]

# GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

## Personal Data as defined in GDPR

- Name and surname
- Home address
- Email address
- Identification card number
- Location data (for example on a mobile phone)
- Internet Protocol (IP) address
- ...

*§ Articles 2, 4(1) and(5) and Recitals (14), (15), (26), (27), (29) and (30)*

## Sensitive Personal Data as defined in GDPR

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
- Trade-union membership
- Genetic data, biometric data processed solely to identify a human being
- Health-related data
- Data concerning a person's sex life or sexual orientation

*§ Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56)*

# GDPR Enforcement Tracker

This website contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any [indication of further GDPR fines and penalties](#).

Show  entries

Search:

Filter by country:



Filter by violation (Art.):

All	5	6	7	9
12	13	14	15	17
18	21	24	25	28
31	32	33	34	35
36	37	58	83	

Country	Authority	Date	Fine [€]	Controller/Processor	Quoted Art.	Type	Summary	Infos
 UNITED KINGDOM	Information Commissioner (ICO)	2019-07-08	204,600,000	British Airways	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other member states have made their representations. The ICO issued a notice of its intention to fine British Airways £183.39M for GDPR infringements which likely involve a breach of Art. 32 GDPR. The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018. The ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information.	<a href="#">link</a>
 UNITED KINGDOM	Information Commissioner (ICO)	2019-07-09	110,390,200	Marriott International, Inc	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	Please note: This fine is not final but will be decided on when the company and other involved supervisory authorities of other member states have made their representations. The ICO issued a notice of its intention to fine Marriott International Inc which relates to a cyber incident which was notified to the ICO by Marriott in November 2018. GDPR infringements are likely to involve a breach of Art. 32 GDPR. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents. It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.	<a href="#">link</a>
 FRANCE	French Data Protection Authority (CNIL)	2019-01-21	50,000,000	Google Inc.	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing	The fine was imposed on the basis of complaints from the Austrian organisation "None Of Your Business" and the French NGO "La Quadrature du Net". The complaints were filed on 25th and 28th of May 2018 - immediately after the GDPR became applicable. The complaints concerned the creation of a Google account during the configuration of a mobile phone using the Android operating system. The CNIL imposed a fine of 50 million euros for lack of transparency (Art. 5 GDPR), insufficient information (Art. 13 / 14 GDPR) and lack of legal basis (Art. 6 GDPR). The obtained consents had not been given "specific" and not "unambiguous" (Art. 4 nr. 11 GDPR).	<a href="#">link</a>
 ITALY	Italian Data Protection Authority (Garante)	2020-01-15	27,800,000	TIM (telecommunications operator)	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing	Between January 2017 and 2019, the data protection authority received hundreds of notifications, in particular concerning the receipt of unsolicited commercial communications made without the consent of the data subjects or despite their registration in the public register of objections. Furthermore, irregularities in data processing in connection with competitions were also complained about. In addition, incorrect and non-transparent information on data processing was provided in Apps provided by the Company and invalid methods of consent were used. In some cases, paper forms requesting one single consent were used for various purposes, including Home License Privacy Impri	<a href="#">link</a>

## PCI DSS

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data.

# PCI DSS Requirements

Goals	Requirements
Secure Network and Systems	Firewall; No default credentials
Protect Cardholder Data	Protect stored data; encrypt transmissions
Vulnerability Management	Anti-Malware/-Virus; Secure Development
Strong Access Controls	Need-to-know access; Authentication; Restrict physical access
Monitoring & Testing	Monitor network and data access; Test systems/processes
Security Policy	Maintain Information Security policy for all personnel



# Cryptographic Failures

- Clear text data transmission (e.g. HTTP, SMTP, FTP)
- Using old or weak cryptographic algorithms or protocols
- Using default crypto keys or generate/re-use weak ones
- Lack of proper key management or rotation
- Crypto keys are checked into source code repositories
- No enforcement of encryption, e.g. missing security directives or headers

**i** *External internet traffic is hazardous. Verify all internal traffic, e.g., between load balancers, web servers, or back-end systems.*

- Insufficient certificate and trust chain validation
- Ignoring, reusing or generating insecure initialization vectors for the cryptographic mode of operation
- Using an insecure mode of operation such as ECB
- Not using authenticated encryption when appropriate
- Use passwords as cryptographic keys in absence of a password base key derivation function
- Using insecure randomness functions or seed them weakly
- Using deprecated (e.g. MD5 or SHA1) or [non-cryptographic hash functions](#) or deprecated cryptographic padding methods (e.g. PKCS number 1 v1.5)
- Allow cryptographic error messages or side channel information to become exploitable, for example in the form of padding oracle attacks

# Data Factors

## A02:2021 – Cryptographic Failures

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences
29	46.44%	4.49%	7.29	6.81	79.33%	34.85%	233,788

# Prevention

- Classifying data processed, stored, or transmitted by an application
- Identify sensitive data according to privacy laws, regulatory requirements, or business needs
- Not storing sensitive data unnecessarily and discarding it as soon as possible
- Encrypting all sensitive data at rest
- Ensuring up-to-date and strong standard algorithms, protocols, and keys are in place while using proper key management


- Encrypting all data in transit with secure protocols (e.g. TLS with [forward secrecy \(FS\)](#) ciphers), cipher prioritization by the server, and secure parameters
- Enforcing encryption with directives like [HTTP Strict Transport Security \(HSTS\)](#)
- No caching of responses that contain sensitive data
- Applying required security controls as per the data classification
- Not using legacy protocols (e.g. FTP and SMTP) for transporting sensitive data
- Storing passwords using strong adaptive and salted hashing functions with a work factor (delay factor)
- Verifying independently the effectiveness of configuration and settings

# Information Classification

Class	Description	Examples
<b>Public</b>	Information without any confidentiality requirements.	User documentation, news, press releases, lunch menus
<b>Internal</b>	Common information inside an organization.	Memos, system documentation or meeting minutes
<b>Confidential</b>	Information or compartmental data with restricted access. Disclosure might induce damage.	Customer, HR, financial or PII data; source code, credentials, logfiles
<b>Secret</b>	Highest confidentiality and integrity requirements. Damaging to organization if	Business secrets, secret formulae,

## Exercise 6.1

For each classification level decide if the listed practices should be allowed (✓) or strictly forbidden (✗). Use footnotes to describe preconditions (if necessary).

Practice	Public	Internal	Confidential	Secret
Publish on Internet				
Publish on Intranet				
Print on 				
Share with third parties				
Copy to USB key				

## Exercise 6.2

For each classification level define restrictions (●) and/or recommendations (○) for the listed lifecycle phases.

Phase	Public	Internal	Confidential	Secret
Permanent storage				
Transfer (internal network)				
Transfer (public network)				
Disposal				



# HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS. It also prevents HTTPS click through prompts on browsers.

## Example

```
Strict-Transport-Security: max-age=16070400; includeSubDomains
```

## Secure Cryptographic Storage Design


- Only store sensitive data that you need
- Use strong approved Authenticated Encryption
- Store a one-way and salted value of passwords
- Ensure that the cryptographic protection remains secure even if access controls fail
- Ensure that any secret key is protected from unauthorized access
- Follow applicable regulations on use of cryptography

## Perfect Forward Secrecy (PFS)

Perfect forward secrecy means that a piece of an encryption system automatically and frequently changes the keys it uses to encrypt and decrypt information, such that if the latest key is compromised, it exposes only a small portion of the user's sensitive data. Encryption tools with perfect forward secrecy switch their keys as frequently as every message in text-based conversation, every phone call in the case of encrypted calling apps, or every time a user loads or reloads an encrypted web page in his or her browser.

**i** Examples of crypto protocols (used for instant messaging conversations) providing PFS are [OTR \(Off-the-record\) Messaging](#) and [Double Ratchet](#) (used within [Signal](#)).

## Best Practices

Scenario	Practice	 Length
Key exchange	Diffie-Hellman	2048+ bits
Message Integrity	HMAC-SHA2	-
Message Hash	SHA2	256 bits
Asymmetric encryption	ECC (Curve25519), RSA	2048 bits (RSA)
Symmetric-key algorithm	AES	128-256 bits
Password Hashing	Argon2id, scrypt, PBKDF2	-

## Exercise 6.3 (🏠)

1. Access a confidential document (★)
2. Retrieve as many clear text user passwords as you can (★★★★)
3. Visit the Token Sale page before it officially goes live (★★★★★)

### Bonus exercises on cryptography (*optional*)

4. Retrieve both the 🐰 easter eggs (★★★★)
5. Solve the steganography challenge (★★★★)
6. Solve the non-existent challenge #999 (★★★★★)