Communication

International data protection laws causing threat for multinational communication company's

Case Study

COMP3721 – Cybersecurity & Information Security

Developed For: Dr Elena Sitnikova

Chief Executive Officer

Approved By: Brenton Borgman

Quality Manager

Developed By: Elie Kadi, kadi0027

Chief Information Security Officer

Version: 1

Date: 15/04/2025

Document History

Release	Date	Description
v1	15/04/2025	Final submission

Table of Contents

Table of Figures

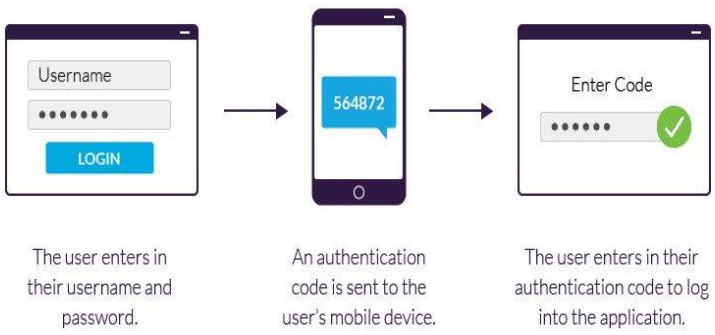

Figure 1: Example of Optus' two factor authentication process (Imperva, 2019)

Table of Tables

GDPR fines	
Tier 1 penalty	Tier 2 penalty
Maxed out at $20,000,000	4% of company's revenue

Table 1: GDRP fines (Worfold, B, 2018)

Business Size	Typical Cost (USD)
Micro Business (<10 employees)	$1,000 – $3,000
Small Business (10-50 employees)	$3,000 – $10,000
Medium Business (50-250 employees)	$10,000 – $50,000

Table 2: Audit costs (ridgewise, 2024)

Training Format	Cost Implications	Benefits	Limitations
Off-the-shelf Programs (Online Courses, Webinars, etc.)	– Affordable, often priced per user or as a yearly subscription (e.g., $100-$500/user/year) – No venue or travel costs	– Easy to deploy with minimal setup – Flexible, self-paced learning	– Limited customization to specific company needs – May lack interactivity and real-world application
Custom In-House Training	– Higher costs due to content development and staff involvement (cost varies significantly) – Potential additional costs for materials and technology	– Tailored to organizational needs and security risks – Allows for company-specific scenarios and policies	– Time-consuming to develop; requires expertise – May require dedicated training personnel
Simulated Exercises	– Resource-intensive; costs may include tech, environment setup, and facilitation fees – Potentially $5,000+ per session	– Realistic, hands-on experience in a controlled setting – Builds readiness through real-world scenarios	– Requires careful scheduling and resource allocation – Higher costs; may disrupt daily work schedules
Blended Learning Programs	– Variable costs based on in-person and online elements (e.g., $500-$2,000 per participant) – Costs for venue, technology, and instructors	– Combines flexibility with hands-on components – Offers structured progression with feedback	– Coordination of both online and in-person sessions required – Typically requires longer training durations

Table 3: Costs, pros and cons to different cybersecurity training (*Bui, S, 2024*)

Introduction

- Communications businesses often lack knowledge behind international data protection laws.
- Communications companies worldwide are breaching these laws.
- These international laws need to be complied with to avoid sanctions and help prevent cyberattacks.

Purpose

- To educate the communications sector about the potential risks of these international laws being breached and not implemented.
- To advocate change in these companies, adhere to these laws and inform them of ways to do so to avoid sanctions and cyberattacks.

Scope

- The document covers different ways to adhere to international data protection laws and standards as well as upholding the ethics of the company.
- A range of sources and examples are used to show how this can be done effectively.

References

This section contains reference information that may be useful in understanding this document's content.

Referenced Acronyms

The following acronyms are used within this document.

Acronym	Expansion
2FA	Two factor authentication
GDPR	General Data Protection Regulation
IBM	International business machines
MFA	Multi factor authentication

Referenced Documents

The following documents, including industry standards, have been used in the development of this document.

Id	Expansion
1.	Australian Cyber Security Centre. (2023). Multi-factor authentication. Australian Signals Directorate. https://www.cyber.gov.au/protect-yourself/securing-your-accounts/multi-factor-authentication
2.	*Bui, S. (2024, November 21). Cyber Security Awareness Training Cost Guide for 2024. F. Learning Studio. https://flearningstudio.com/cyber-security-awareness-training-cost/*
3.	Cybersecurity Awareness and Practices: Survey Results. (2024). Techbehemoths.com. https://techbehemoths.com/blog/cybersecurity-awareness-practices-survey-results
4.	*Data Breaches: Understanding the Business Impact | Baldwin*. (2025, February 25). The Baldwin Group. https://baldwin.com/insights/understanding-the-business-impact-of-data-breaches/
5.	Denayer, D. (2021, September 27). Use Two-factor authentication to comply with GDPR. OneSpan. https://www.onespan.com/blog/use-two-factor-authentication-comply-gdpr
6.	*Dictionary.com | Meanings & Definitions of English Words*. (2023). Dictionary.com. https://www.dictionary.com/browse/law#google_vignette
7.	Gov.UK. (2024). Cyber security skills in the UK labour market 2024. GOV.UK. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024
8.	Imperva. (2019). What is Two Factor Authentication | Pros and Cons of 2FA | Imperva. Learning Center. https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/
9.	Labs, K. (2024, January 23). 2025 Security Awareness Training Statistics. Keepnet Labs. https://keepnetlabs.com/blog/security-awareness-training-statistics
10.	Matthew Kosinski. (2024, May 24). *What is a Data Breach?* Ibm.com. https://www.ibm.com/think/topics/data-breach
11.	Partida, D. (2024, January 22). How often should security audits be? Levelblue.com. https://levelblue.com/blogs/security-essentials/how-often-should-security-audits-be
12.	*PrivacyEngine*. (2024, September 24). PrivacyEngine Data Protection Software and Consultancy. https://www.privacyengine.io/resources/glossary/user-consent/

Id	Expansion
13.	Queensland Government. (2022). *Optus data breach*. Queensland Government. https://www.qld.gov.au/community/your-home-community/cyber-security/cyber-security-for-queenslanders/case-studies/optus-data-breach
14.	ridgewise. (2024, October 15). Average Cost of an Audit for a Small Business: Budgeting and Benefits Explained - Ridge wise. Ridge Wise - MAKE ACCOUNTING SIMPLE with US. https://ridgewise.com/average-cost-of-an-audit-for-a-small-business/
15.	Shopify API. (2024, November 2). How to estimate budget for security features in a mobile app? BusinessDojo. https://dojobusiness.com/blogs/news/mobile-app-security-budget-estimation
16.	St.John, M. (2024, February 28). Cybersecurity Stats: Facts and Figures You Should Know – Forbes Advisor. Forbes. https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/
17.	Team ZCySec. (2023, June 27). *What Is Cyber Security Audit? What It Is, & Why Is It Important?* Zcybersecurity.com. https://zcybersecurity.com/what-is-cyber-security-audit/
18.	Telstra Standard Terms General Terms. (2024). https://www.telstra.com.au/content/dam/tcom/personal/consumer-advice/pdf/consumer/telstra-standard-terms-general-terms-22122024.pdf
19.	Turnbull, T. (2022, September 29). Optus: How a massive data breach has exposed Australia. *BBC News*. https://www.bbc.com/news/world-australia-63056838
20.	Two Factor Authentication. (2025). Optus.com.au. https://sms.optus.com.au/docs/en/solution-sheets/2fa/
21.	*Understanding the Costs of Multi-Factor Authentication - Trout Blog*. (2025). Trout.software. https://www.trout.software/resources/tech-blog/understanding-the-costs-of-multi-factor-authentication
22.	*What are Terms and Conditions in a Contract? (2025). Icertis.com. https://www.icertis.com/contracting-basics/what-are-terms-and-conditions/*
23.	Wolford, B. (2018, November 7). What Is GDPR, the EU's New Data Protection Law? GDPR.EU. https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

Glossary of Terms

The following terms are used within this document and as such, they have been defined in a glossary for the benefit of audience members not familiar with these technical terms.

Term	Definition
Audit	A comprehensive evaluation of an organization's computer systems, networks, policies, and procedures (Team ZCySec, 2023).
Authentication	The act or process of establishing identity and verifying permission to access an electronic device or computer network (dictionary, 2023).
Cyberattack	An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network (dictionary, 2023).
Data Breach	Any security incident in which unauthorized parties' access sensitive or confidential information (Matthew Kosinski, 2024).

Term	*Definition*
Declaration	A document embodying or displaying an announcement or proclamation (dictionary, 2023).
Fraud	Illegal online activities that deceive people or organizations (dictionary, 2023).
Identity theft	The fraudulent appropriation and use of someone's identifying or personal data or documents, as a credit card (dictionary, 2023).
Law	The principles and regulations established in a community by some authority and applicable to its people, whether in the form of legislation or of custom and policies recognized and enforced by judicial decision (dictionary, 2023).
Terms and conditions	Legally enforceable agreements between a business and its users that define the rules for using a product, service, or website (Icertis, 2025).
User consent	The informed, explicit, and voluntary agreement by a user to the processing of their personal data (PrivacyEngine, 2024).

Problem Decomposition

Problem Statement:

International data protection laws causing threat for multinational communication companies.

There are five specific topics that contribute or inform your company about the problem, which are the following:

1. The GDPR

2. Recent communications sector cyberattack on Optus

3. Staff and user accounts, which contains private information, do not use authentication processes

4. Companies do not offer clear options for customers to consent to data

5. Potential consequences with not fixing the following issues

(1) The GDPR

- The GDPR is Europe's new data privacy and security laws (Worfold, B, 2018).
- The GDPR is the toughest privacy and security law in the world (Worfold, B, 2018).
- There are more laws in place in Europe under this protection then anywhere in the world (Worfold, B, 2018).

(2) Recent communications sector cyberattack on Optus

- In 2022, one of the largest communication companies Optus had their data breached due to a cyberattack (Turnbull, T, 2022).

- 10 million Optus customers had personal data stolen including names, birthdays, home addresses, phone and emails contacts and passport and driver's license numbers (Turnbull, T, 2022).
- 2.8 million people were at a high risk to have identity theft and fraud due to passport and licence numbers being breached (Turnbull, T, 2022).
- This attack has costed Optus $1.5 billion in brand value (Queensland Government, 2022).
- This cyberattack is something that has increased security and laws behind communications businesses, to help prevent future data breaches.

(3) Staff and user accounts, which contains private information, do not use authentication processes

- 2023 saw a 72% increase in data breaches since 2021, which held the previous all-time record (St.John, M, 2024).
- Hence, your systems and information safety should be taken with high precaution.
- One of the general GDPR requirements is for staff members that deal with medium to high-risk data to use authentication processes (Denayer, D, 2021).
- The main effect of this problem is your systems getting hacked into easily, and sensitive private data being leaked.
- The data that can be leaked can be catastrophic which could include peoples phone numbers, emails, home addresses, and even credit card details

(4) Companies do not offer clear options for customers to consent to data

- This is a violation of the GDPR conduct, which could lead to your company being heavily fined.
- It is not ethically correct to not make the consent options more visible and accessible.
- Customers should have the right to see what they are consenting to.

(5) Potential consequences with not fixing the following issues

- According to IBM's 2024 Cost of a Data Breach Report, the global average cost of a data breach reached increased 10 percent from 2023, reaching $4.88 million (Baldwin, 2025).
- Keeping data and information in your company confidential to the user is priceless.
- If this is not done, the company image can get a bad reputation, which can lead to losing customers.
- Ethically as a business, looking at the customers point of view and making their security of sensitive information priceless is a priority.
- The GDPR can potentially fine your company for violating certain protection laws and conducts (Worfold, B, 2018).
- Financial penalties can be found in table 1.
- Users could potentially get compensation money for misconduct of their information if their data is breached (Worfold, B, 2018).

Identified Solutions

2FA

- Other similar companies in the communications sector such as Optus and Vodaphone have implemented different strategies and procedures within their system.
- Both companies use 2FA not only for staff but also customers' accounts.
- Optus' 2FA they use is a text message containing a 6-digit code that can be entered before entering the system, as shown in figure 1 (Optus, 2025).
- This 6-digit code can only be entered during a certain time period before it expires, hence making these accounts even more secure (Optus, 2025).
- An easy way to solve the 2FA issue would be before you are granted access to login, the staff member or customer receives a time sensitive text message with a code.
- Before they log into their account they have to enter this 6-digit code into the system within 5 minutes to gain access to the system.
- This makes the customers data much less hackable and more safe and secure within your company.

MFA

- MFA is a security measure that requires two or more proofs of identity to grant you access (Australian Cyber Security Centre, 2023).
- This keeps staff and user accounts more secure than just using 2FA.
- MFA can include implementing a pin or secret question, fingerprint id, face id, and authentication mobile apps (Australian Cyber Security Centre, 2023).

Training and education

- TechBehemoths surveyed 1,585 IT companies across 62 countries from January 15-22, 2024 (Techbehemoths, 2024).
- Techbehemoths found that 69.1% of Employees Receive Regular Cybersecurity Awareness Training (Techbehemoths, 2024).
- That's over two thirds of companies that are investing time and money into their employees' gaining knowledge on cybersecurity awareness.
- The UK government have stated that 44% of businesses have skill gaps in technical areas (Gov.uk, 2024).
- More professional extensive training behind information security and procedures that follow this should be covered with all staff members that deal with medium to high level data.
- This means that staff members are more likely to follow procedures that make your systems less hackable.
- Keepnet labs, a cybersecurity training company has stated that Cyber security awareness training leads to a 70% reduction in security-related risks in 2023 (Keepnet Labs, 2024).
- Conducting in cybersecurity training for your business also keeps staff accountable to these professional standards and practises.

User consent

- Big communications companies such as Telstra, Optus and Vodaphone make their consent options and consent declaration documents accessible on their website and in their accounts.
- This means that customers can review these declarations at any given time.
- For example, Telstra also text, email, and use the Telstra app to communicate any changes to the terms and conditions (Telstra, 2024).
- This upholds the ethics of the company and gives customers a chance to read and re-evaluate the terms and conditions if needed.
- Before users create accounts, it is essential that you provide a consent feature.
- This could be a tick box or a signed declaration.
- All consenting documents should be accessible to users for them to read and understand before consenting.
- If changing any terms and conditions or declarations that the user has consented to, it is essential that your company contacts the user to make them aware of these changes.

Audits

- Regular audits such should be done at a bare minimum twice a year (Partida, D, 2024).
- Audits should be aimed to do more frequently to quarterly or monthly (Partida, D, 2024).
- This ensures that the correct information and cybersecurity measures are taken which reduces the chances of cyberattacks (Partida, D, 2024).

Cost/time estimates

- Implementing 2FA can cost between $3,000 and $10,000 as a one-off cost (Shopify API, 2024).
- MFA apps such as Cisco DUO or Okta cost around $3 - $10 per user (Trout, 2025).
- Creating better consent features just costs staff members times.
- They would need to spend time creating and implementing these better consent features which should only take them between 1-2 days if done correctly.
- Audit costs for various business sizes can be found in table 2.
- Costs, pros and cons to different cybersecurity trainings can be shown in table 3.
- These in person cybersecurity sessions can be over multiple days/sessions for staff members.
- Basic level online cybersecurity training can also be conducted within a week.

Conclusions

- Ordering regular audits, creating better consent features, implementing a 2FA or MFA for accounts, and having extensive cybersecurity training is something that will cost your company time and money.
- Implementing the following will reduce the chances of cyber attacks and also reduce the chances of receiving fines from the GDPR which will save the company lots of money in the long run.