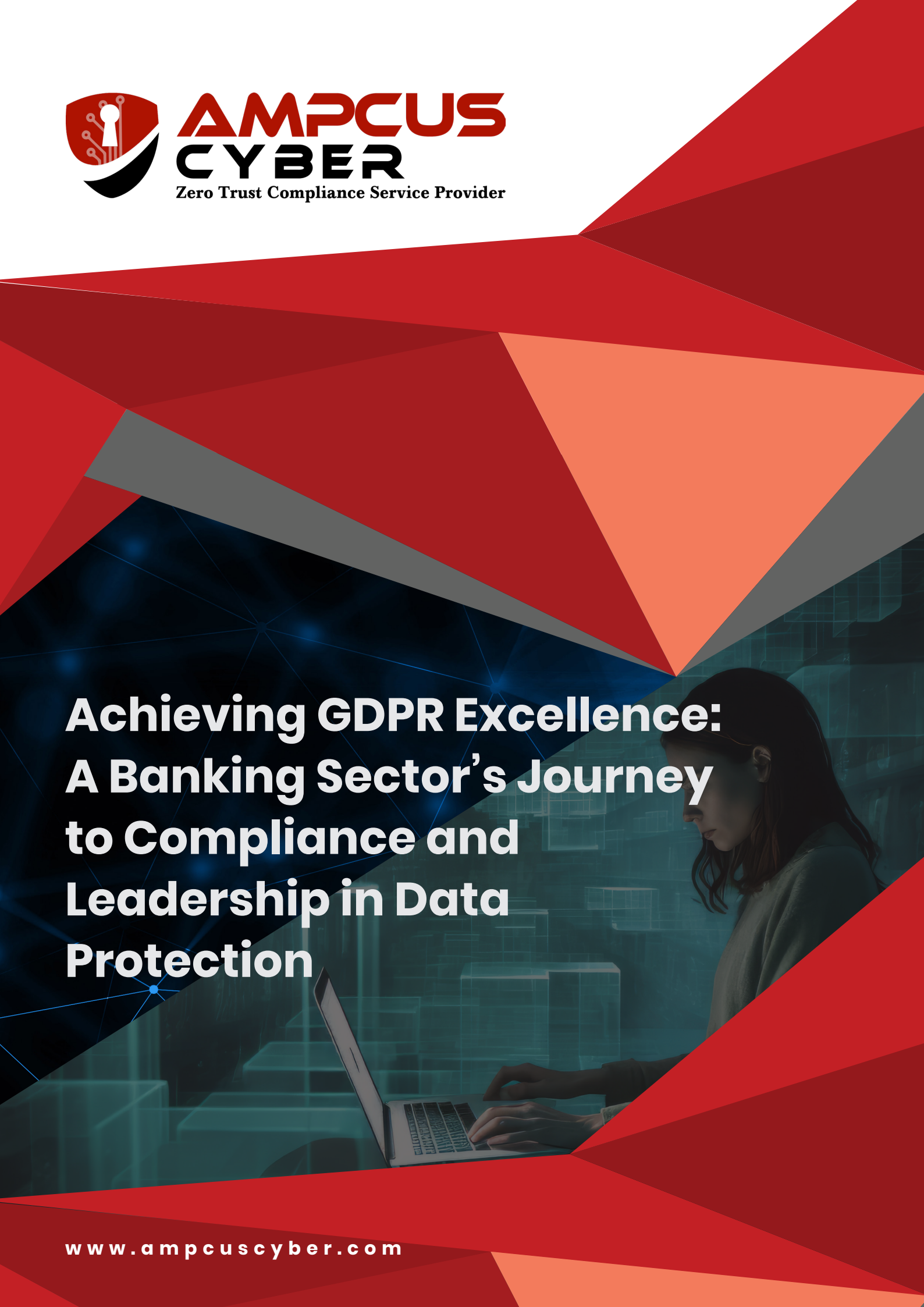
AMPCUS CYBER

Zero Trust Compliance Service Provider

Achieving GDPR Excellence: A Banking Sector's Journey to Compliance and Leadership in Data Protection



www.ampcuscyber.com

GDPR COMPLIANCE CASE STUDY

How a leading European financial institution embarked on a journey to achieve GDPR compliance, strengthening its data protection practices and fostering customer trust.

SUMMARY

Customer: European Financial Institution
Industry: Banking Sector

CHALLENGES

Multiple Legacy Systems to be updated to meet GDPR requirements. Requirement was to ensure GDPR compliance among numerous third-party data processors as well.

RESULTS

By proactively addressing GDPR compliance and adapting to the evolving cybersecurity landscape, the bank positioned itself as a leader in data protection within the banking industry.

INTRODUCTION

In this case study, we delve into the journey of achieving and maintaining compliance with the General Data Protection Regulation (GDPR) by Ampcus Cyber for a leading European financial institution. We hope to take you through the entire process, highlighting the challenges faced and our unique solutions to overcome them!

BACKGROUND

Ampcus Cyber received an RFP from leading European financial institution, for a comprehensive GDPR compliance assessment. The bank had recently launched a digital transformation initiative, introducing new online banking services and mobile applications, which raised concerns about data protection and privacy. As the project progressed, the bank sought end-to-end support in achieving and maintaining GDPR compliance across all its entities. With a strong commitment to customer trust and regulatory compliance, the bank embarked on this journey to strengthen its data protection posture considering its expanding digital offerings.

CHALLENGES

Prior to initiating the project for GDPR compliance, the bank faced several challenges:

Third-Party Data Sharing: The bank's new digital services relied on partnerships with third-party providers, raising concerns about data sharing and potential breaches.

Data Subject Rights & Consent Management: The introduction of new digital channels made it challenging to efficiently handle data subject rights requests. Obtaining and managing valid consent for data processing across multiple digital platforms proved difficult.

Data Breach Notification: Establishing effective processes for timely data breach notification within the 72-hour GDPR timeframe was a challenge.

Legacy Systems: Updating multiple legacy systems to meet GDPR requirements complicated the bank's digital transformation efforts.

Third-Party Compliance: Ensuring GDPR compliance among numerous third-party data processors added complexity to the bank's compliance journey.

GDPR COMPLIANCE JOURNEY

To address the challenges posed by the bank's digital transformation initiative and ensure compliance with GDPR, Ampcus Cyber embarked on a comprehensive GDPR compliance journey.

Initiation and Leadership: Ampcus Cyber initiated the GDPR compliance project with the full support of the bank's senior management. A dedicated Data Protection Steering Committee was formed to oversee the implementation process and ensure alignment with business objectives. The committee was made aware of the gaps and vulnerabilities identified during the initial assessment stage and the effort required to mitigate them.

Data Mapping and Inventory: Ampcus Cyber conducted a thorough data mapping exercise to identify and categorize personal data processed by the bank across all systems and departments, including the new digital platforms. A data flow map was created to visualize data processing activities and identify potential risks.

Data Protection Impact Assessment (DPIA): Given the high-risk nature of the bank's data processing activities, particularly with the introduction of new digital services, Ampcus Cyber performed a comprehensive DPIA. The DPIA involved a systematic assessment of the necessity and proportionality of data processing operations, the risks to data subjects' rights and freedoms, and the measures in place to mitigate those risks. The DPIA helped identify areas requiring additional controls and served as a key tool in demonstrating GDPR compliance.

Policy and Procedure Development: Ampcus Cyber developed a robust Data Protection Policy outlining the bank's commitment to data privacy and compliance with GDPR. The policy was supported by specific procedures for data subject rights management, data breach notification, and data retention. These policies and procedures were communicated to all employees and stakeholders, emphasizing their roles and responsibilities in maintaining data protection.

Technical and Organizational Measures: Based on the findings of the data mapping, DPIA, and gap analysis, Ampcus Cyber assisted the bank in implementing appropriate technical and organizational measures. This included measures such as data encryption, pseudonymization, access controls, and data loss prevention solutions. Legacy systems were updated to ensure compliance with GDPR requirements, and third-party data processors were assessed and contractually bound to adhere to GDPR standards.

Data Subject Rights Management: Ampcus Cyber helped the bank establish efficient processes for handling data subject rights requests, such as the right to access, rectify, or erase personal data. This involved automation wherever possible as per the bank's allocated budget like implementing self-service portals, automated workflows, and training customer support teams to handle such requests in a timely and compliant manner.

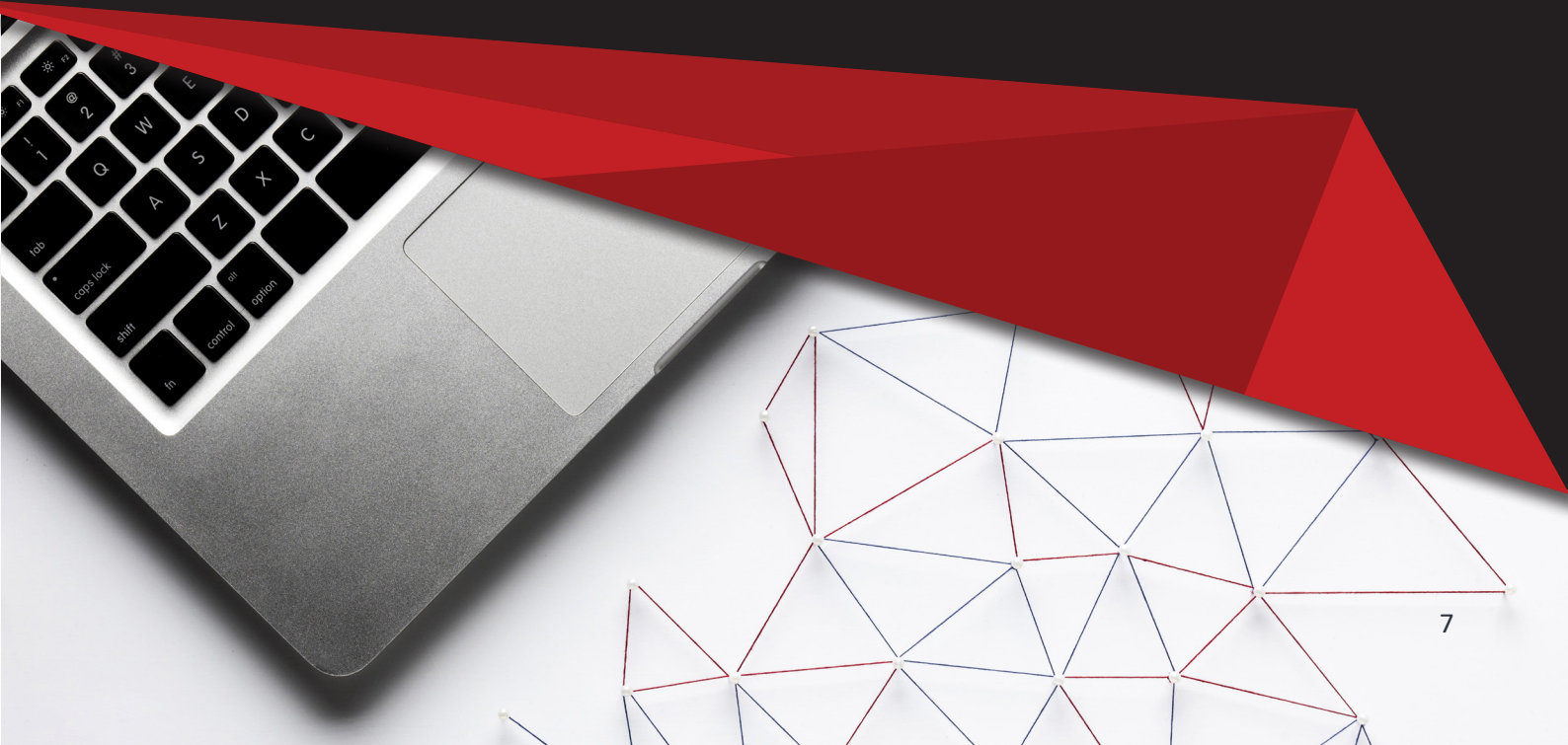
Consent Management: To address the challenges of obtaining and managing valid consent across multiple digital platforms, Ampcus Cyber developed a consent management framework. This framework included clear guidelines for obtaining explicit, freely given, and informed consent from data subjects. Consent forms and privacy notices were reviewed and updated to ensure they were concise, transparent, and easily accessible. Regular audits were conducted to ensure that consent records were accurate, up-to-date, and readily available to demonstrate compliance with GDPR requirements.

Data Breach Notification: Ampcus Cyber developed a comprehensive data breach response plan, outlining the roles and responsibilities of key stakeholders and the steps to be taken in the event of a data breach. The plan included processes for detecting, investigating, and notifying relevant authorities and affected individuals within the 72-hour timeframe mandated by GDPR.

Training and Awareness: Ampcus Cyber conducted tailored training sessions to educate employees on GDPR requirements, data protection best practices, and their specific roles in maintaining compliance. This included specialized training for key personnel, such as data protection officers and IT staff, to ensure a thorough understanding of GDPR obligations.

Ongoing Monitoring and Audits: To ensure continued compliance, Ampcus Cyber implemented an ongoing monitoring program, including regular audits and assessments of the bank's data protection practices. This helped identify any deviations from GDPR requirements and facilitated prompt corrective actions.

A final comprehensive audit was conducted to validate that all identified gaps were effectively remediated, demonstrating Ampcus Cyber's successful achievement of GDPR compliance.



CONCLUSION

The bank was awarded GDPR compliance certification after successfully passing the comprehensive final compliance audit. This validation serves as a true testament to the bank's and Ampcus Cyber's collective efforts throughout this critical project engagement.
The successful implementation of robust GDPR controls has positioned the bank as an industry leader in data protection and privacy within the European financial sector. By proactively adopting a privacy-by-design approach to risk management and compliance, the bank has safeguarded not only its own interests but reinforced its commitment to protecting the interests of its valued customers.

WHAT DID THE BANK ACHIEVE WITH GDPR COMPLIANCE?

Strengthened Data Protection: By aligning with GDPR requirements, the bank significantly fortified its data protection measures, mitigating risks of potential data breaches and ensuring robust safeguards for customer privacy.

Regulatory Compliance: The GDPR implementation enabled the bank to demonstrate comprehensive compliance with the EU's data protection regulations, avoiding potential fines and reputational damages.

Customer Trust and Confidence: The bank's commitment to GDPR compliance reinforced customer trust and confidence in its ability to responsibly handle and protect their sensitive personal and financial information within its digital ecosystems.

USA
Ampcus Cyber Inc., 14900 Conference Centre, Drive Suite #500, Chantilly, VA 20151.

India
Unit No. 601-608, 6th floor Beta Block, Sigma Tech Park, Varthur, Bengaluru - 560 066. Ph No. - (703) 621 - 1318

Philippines
Tower 3, Unit 1914, Grace Residences, Levi Mariano Avenue, Ususan Taguig City, Metro Manila 1632, Philippines

Dubai
Dubai Silicon Oasis, DDP, Building A1, Dubai, United Arab Emirates