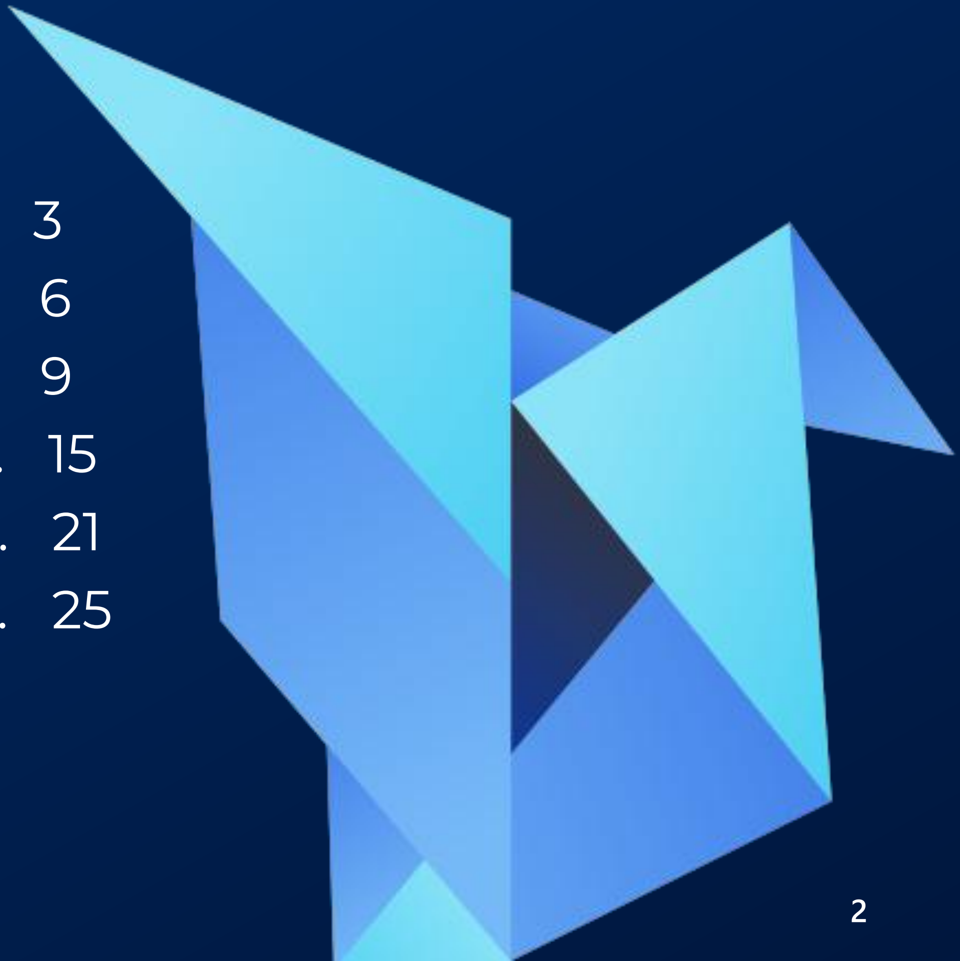
PACIFICA

A NOVENTIQ Company

Personal Data at Risk: Breaches and Protection Methods

Maxim KARMYKOV – Cybersecurity Specialist

Contents



Why It Matters

Today, personal data are not just numbers and letters. They are a valuable asset, comparable to money or even oil.

Each of us leaves a digital footprint: on social media, when shopping, or while using online services. And any data breach can have serious consequences – from financial losses to loss of customer trust.

Statistics show that more than **60% of companies have faced a data breach at least once.** That's why information protection is not only an IT issue – it is a matter of reputation and business survival.

What Are Personal Data?

- **Personal data** are any information about an individual (the data subject) that allows them to be identified directly or indirectly. This includes: full name, passport number, address, date of birth, employment details, health records, as well as biometric data such as photographs or fingerprints.
- The key difference from **confidential information** is that personal data are always linked specifically to an individual. Confidential information, on the other hand, is a broader term.

Categories of Personal Data

- **General:** full name, date of birth, place of residence, phone number, photograph, email address.
- **Sensitive:** political views, racial or ethnic origin, religious and philosophical beliefs.
- **Biometric:** fingerprints, DNA, voiceprint, iris pattern.
- **Numeric identifiers:** passport or ID number, bank account and card numbers, individual identification number (IIN).

Rising Cyberattacks and Data Breaches

- The number of cyberattacks worldwide increases by 20-30% each year.
- Data breaches are becoming increasingly large-scale, with tens of millions of records ending up publicly exposed. The average cost of a security incident for a company exceeds $4 million (according to IBM).
- Main causes include phishing, weak passwords, employee mistakes, and software vulnerabilities.
- A recent trend is the rise of cyberattacks targeting government institutions, banks, and critical infrastructure.

Top Data Security Threats

- **Hacker Attacks:** database breaches, theft of logins and passwords.
- **Phishing and Social Engineering:** tricking victims into voluntarily revealing their data.
- **Internal Leaks:** employee mistakes or deliberate actions.
- **Insufficient Service Protection:** weak passwords, lack of encryption.

Typical Cyberattack Scenarios

- **Phishing**
  An employee receives an email from a “bank” or “colleague,” opens an attachment → a virus is installed → the attacker gains access to corporate email and documents.
- **Employee Data Leak**
  A manager downloads a client database onto a USB drive for “working from home convenience” → the USB drive is lost → data becomes publicly exposed.
- **Attack via Contractor**
  A supplier connects to the company network via VPN → their account is compromised → the attacker gains access to the company’s internal systems.
- **Social Engineering**
  A call “from IT support”: the employee is asked for their password for verification → the account is intercepted → data and money are stolen.

Impact of Personal Data Leaks

- **For Companies:** financial losses, fines, lawsuits.
- **For Customers:** fraud, identity theft, loss of money.
- **For the Brand:** loss of trust and reputational damage.

For example, in recent years, many large companies have experienced high-profile data breaches, and rebuilding their customers’ trust took years.

Common Data Protection Mistakes by Companies

- Relying solely on antivirus
- Ignoring internal risks
- Lack of employee training
- Underestimating regulatory requirements
- Fragmented protection
- Excessive default access

User Behavior Is the Biggest Risk!

- **80% of data breaches** are caused by human error.
- Employees use **weak** or identical passwords.
- They send work documents via **personal email** and **messaging apps**.
- They open **phishing emails** and **attachments** without verifying the sender.
- They often break security rules **out of haste** or **convenience**.

Even the most advanced technologies are ineffective without employee training and strict corporate security policies.

Real Cases of Personal Data Breaches Worldwide

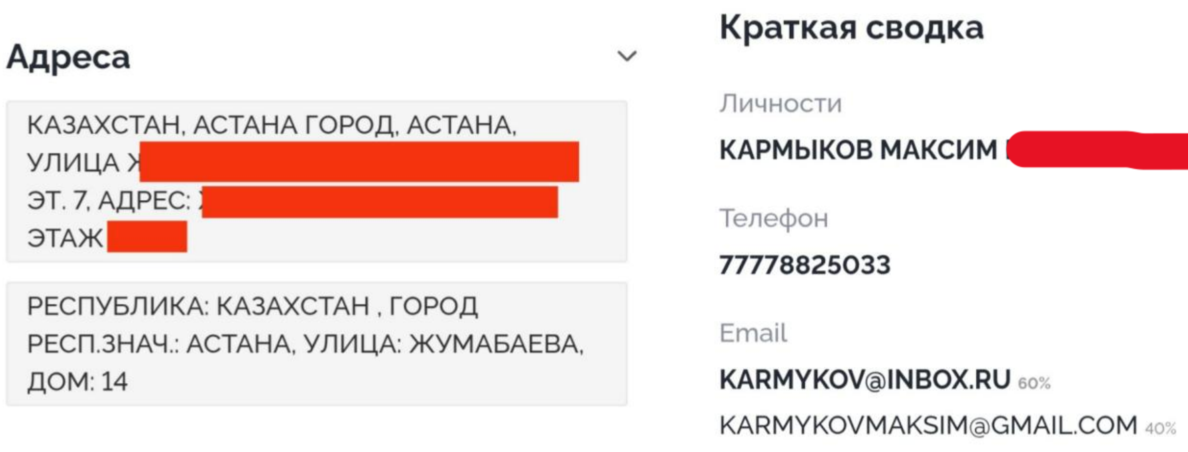
- **Mother of All Breaches (MOAB)** – *January 2024*
  The largest data breach in history: 26 billion records collected from multiple sources (Tencent QQ, Weibo, Myspace, etc.).
- **National Public Data** – *January 2024*
  2.9 billion records, including addresses, Social Security numbers, and other personal information. The breach occurred at a U.S. data broker.
- **Alibaba Cloud** – *July 2022*
  1.1 billion records leaked via a cloud service: names, IDs, phone numbers, addresses, and criminal records.
- **LinkedIn** – *June 2021*
  700 million user profiles put up for sale: names, emails, phone numbers, and other contact information.

Real Cases of Personal Data Breaches in Kazakhstan

- **Personal Data Breach of 16.3 Million Citizens – June 2025** – One of the largest personal data breaches in Kazakhstan's history.
- **Microfinance Platform Data Leak – March 2024** - Over 2 million client records, including data of Kazakh citizens as well as information from Russia, the Philippines, and Vietnam, were found publicly exposed.
- **JSC Incident (2021-2022)** – Unauthorized access was detected in the infrastructure of telecom operators, the Unified National Pension Fund (ENPF), and Air Astana. The cause was weak security in the JSC; the incident is being investigated by the National Security Committee (KNB).

Personal Data Breaches Are Closer Than You Think

- Personal data regularly becomes publicly accessible.
- There are even **informal channels**, such as Telegram bots, where anyone can check at least some information about themselves.
- This highlights the **scale of the problem**: if such data is available in a messaging app, imagine what it could mean in the hands of cybercriminals.



Адреса

КАЗАХСТАН, АСТАНА ГОРОД, АСТАНА, УЛИЦА [redacted]
ЭТ. 7, АДРЕС: [redacted]
ЭТАЖ [redacted]

РЕСПУБЛИКА: КАЗАХСТАН , ГОРОД РЕСП.ЗНАЧ.: АСТАНА, УЛИЦА: ЖУМАБАЕВА, ДОМ: 14

Краткая сводка

Личности
КАРМЫКОВ МАКСИМ [redacted]

Телефон
77778825033

Email
KARMYKOV@INBOX.RU 60%
KARMYKOVMAKSIM@GMAIL.COM 40%

Ways to Protect Personal Data

How to Protect Yourself? A Comprehensive Approach Is Key:

- **Technical Measures:** encryption, secure communication channels, backup.
- **Organizational Measures:** access control, employee training, process audits.
- **Legal Measures:** compliance with personal data laws, transparent privacy policies.

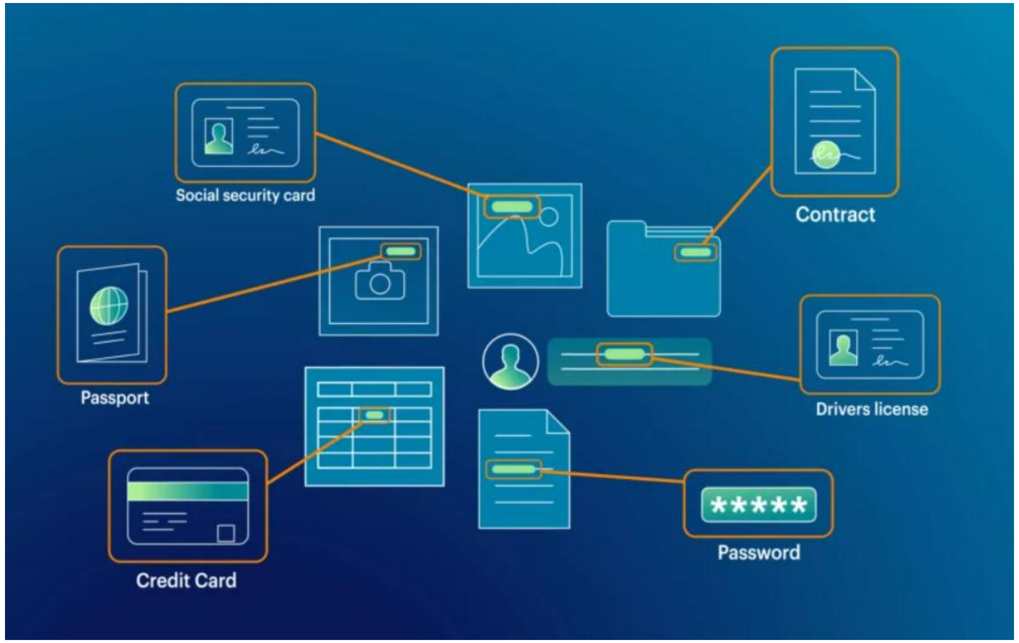
It is important to understand: there is no single "magic button." Protection must be implemented systematically.

Technical Tools for Protecting Personal Data

- DLP (Data Loss Prevention)
- SIEM (Security Information and Event Management)
- NGFW (Next-Generation Firewall)
- PAM (Privileged Access Management)
- EDR/XDR (Endpoint/Extended Detection and Response)
- Encryption and Tokenization
- Backup and BCP (Business Continuity Planning)
- Vulnerability Management Systems

DLP in Action

1. User attempts to send data
2. DLP intercepts the user action
3. Content analysis
4. Matching against security policies
5. System response
6. Security team notification



Technical Tools for Protecting Personal Data

- *«Technical measures are the foundation of protection. But maximum effectiveness is achieved only through a comprehensive approach: technology + processes + training»*

Trellix

Data Loss Prevention

falcongaze

FUDO

SECURITY

CHECK POINT™

FORTINET®

Leadership’s Role

- Strategic decision-making
- Budget allocation
- Fostering a security culture
- Accountability for consequences
- Oversight and monitoring

Data Protection: Looking Ahead

What Lies Ahead?

- Growing role of artificial intelligence – both in cyberattacks and in protection.
- Stricter legislation: governments demand greater accountability from companies.
- Personal data is becoming a new form of capital – managed and protected on par with financial assets.

Tips for Companies and Users

Some practical tips:

- **For companies:** implement an information security policy, train employees, and conduct regular inspections.
- **For users:** use complex passwords, enable two-factor authentication, and be careful with suspicious emails and calls.

PACIFICA: Your Cyber Protection Against Data Breaches

We don’t just put “locks” on your systems – we build a comprehensive protection strategy that:

- **Minimizes data breach risks** – DLP and PAM control access and prevent leaks of critical data.
- **Enables instant response to attacks** – SIEM and XDR detect and respond to incidents in real time.
- **Protects your infrastructure 24/7** – NGFW and EDR block sophisticated cyberattacks both at the perimeter and within the network.
- **Helps avoid fines and reputational damage** – ensures regulatory compliance and protects clients’ personal data.

PACIFICA – *is an integrator that turns a set of solutions into a turnkey, unified data protection ecosystem.*

PACIFICA: Real-World Case

Challenge:

A large financial company faced the risk of confidential employee and customer data being leaked via email and messaging apps.

PACIFICA Solution:

- Implemented a **DLP** system to monitor all data transmission channels.
- Configured security policies: prohibited sending personal data outside the corporate network.
- Trained employees on safe data handling practices.

Result:

- Reduced data leak risk by **80% within the first 3 months**.
- Detected and prevented over **500 attempts of unauthorized data transmission**.
- The company avoided fines and maintained customer trust.

About PACIFICA

TURNOVER
3.0
MILLION $

2
OFFICES

MORE
20
AUTHORIZATIONS
OF VENDORS

>15 YEARS
ON THE
SECURITY
MARKET

20
SPECIALISTS

MORE
100
CLIENTS

ISO
27001
COMPLIANCE

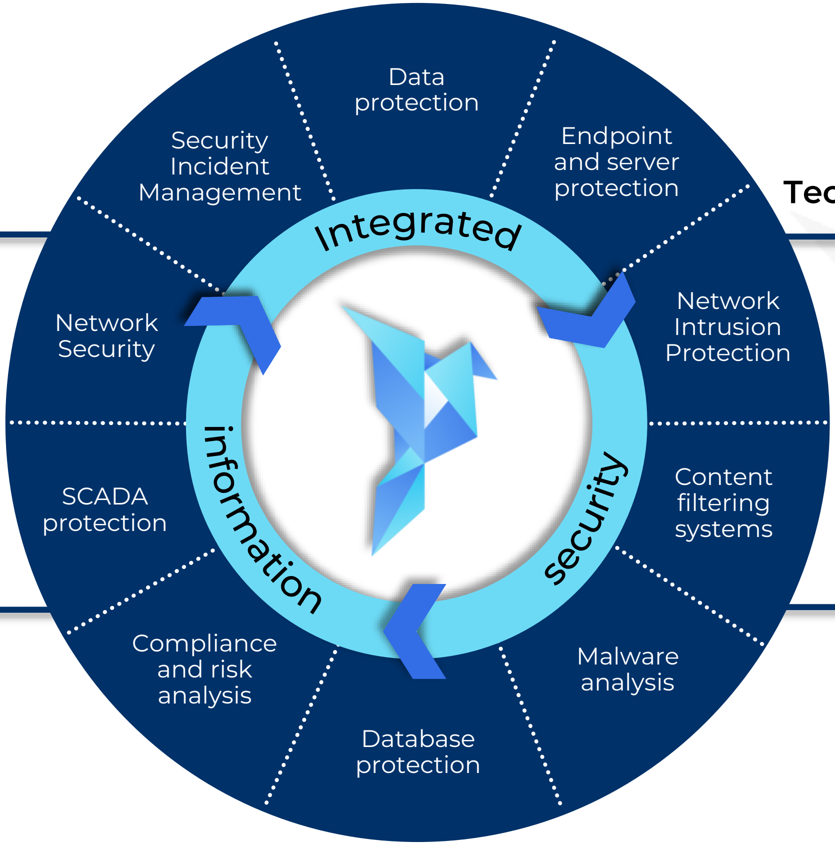
Areas of Activity

Audit and consulting

- Preparation for audit in accordance with international standards (ISO 27001, PA/PCI DSS)
- Information security consulting
- Security analysis (technical audit)

Design and implementation

- Design and implementation of information security systems (ISS)
- Consulting of Security Operation Centers (SOC) construction
- Protection of Data Processing Centers (DPC)


Integrated
information
security
Data protection
Endpoint and server protection
Network Intrusion Protection
Content filtering systems
Malware analysis
Database protection
Compliance and risk analysis
SCADA protection
Network Security
Security Incident Management

Technical support and outsourcing

- Support and maintenance of information security systems (ISS)
- Optimization of cybersecurity infrastructure, cybersecurity outsourcing, cloud information security services

Education services

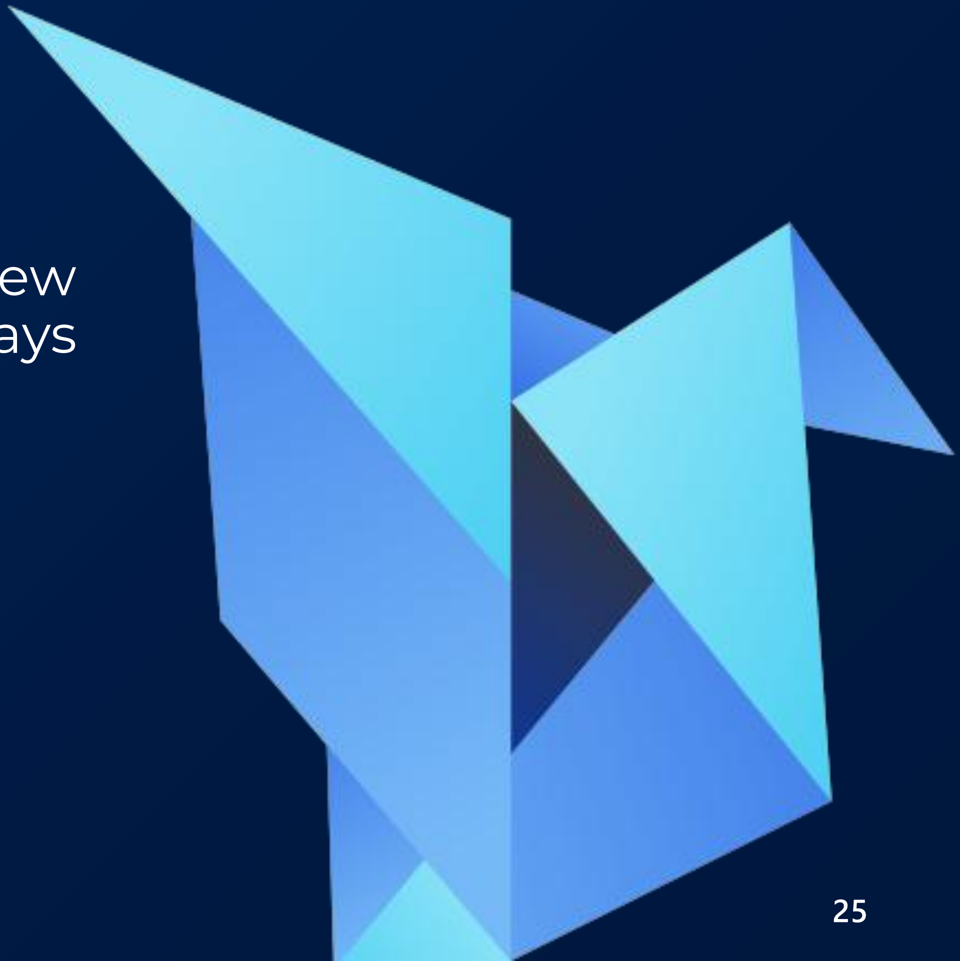
- Conducting trainings and seminars for managers and technical specialists of IS
- Trainings of information security specialists according to author's courses

PACIFICA LLP provides a range of solutions and services that allow our clients to build information security systems from scratch or optimize an existing one

Conclusion

Personal data protection is a continuous process. New threats emerge every day, and companies must always stay one step ahead.

PACIFICA is ready to be your partner in this.



PACIFICA

A NOVENTIQ Company