Polityka Bezpieczeństwa

CKHM spółki z ograniczoną odpowiedzialnością

prowadzącej

Hotelu Malbork**** Centrum Konferencyjne

z siedzibą w Malborku 82-200, przy ul. Parkowa 2

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w CKHM spółce z ograniczoną odpowiedzialnością z siedzibą w Malborku, prowadzącej Hotel Malbork**** Centrum Konferencyjne zwana dalej Polityką Bezpieczeństwa wskazuje sposób postępowania w sytuacji przetwarzania danych osobowych oraz naruszenia bezpieczeństwa tych danych i jest przeznaczona dla osób pracujących przy przetwarzaniu danych osobowych w CKHM spółce z ograniczoną odpowiedzialnością prowadzącej Hotel Malbork**** Centrum Konferencyjne z siedzibą w Malborku 82-200 przy ul. Parkowej 2.

Definicje

1. Ilekroć w niniejszym dokumencie jest mowa o:

    - Polityce bezpieczeństwa – należy przez to rozumieć politykę bezpieczeństwa w zakresie ochrony danych osobowych w **CKHM spółce z ograniczoną odpowiedzialnością** z siedzibą w Malborku (82-200), ul. Parkowa 2, wpisanej do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0001108048, REGON: 528740774, NIP 5792295679, prowadzącej Hotelu Malbork**** Centrum Konferencyjne w Malborku.

    - RODO – należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

    - Administratorze – rozumie się przez to **CKHM spółkę z ograniczoną odpowiedzialnością** z siedzibą w Malborku (82-200), ul. Parkowa 2, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0001108048, REGON: 528740774, NIP 5792295679, prowadzącą Hotel Malbork**** Centrum Konferencyjne z siedzibą w Malborku 82-200 przy ulicy Parkowej 2.

- Podmiocie przetwarzającym (Procesorze) – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

- Stronie trzeciej – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot niż osoba, której dane dotyczą, Administrator, Podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub Podmiotu przetwarzającego mogą przetwarzać dane osobowe.

- Odbiorcy danych – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

- Danych osobowych – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwej do zidentyfikowania osobie fizycznej – należy przez to zrozumieć osobę, którą można pośrednio lub bezpośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

- Przetwarzanie danych – należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nie zautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

- Zbiorze danych – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

- Zgodzie osoby, której dane dotyczą – należy przez to rozumieć dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

- Systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

- Zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- Instrukcja zarządzania systemem informatycznym – należy przez to rozumieć Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w CKHM spółce z ograniczoną odpowiedzialnością prowadzącej Hotelu Malbork**** Centrum Konferencyjne.

2. Obszary przetwarzania danych osobowych:
    - Obszary przetwarzania danych osobowych – miejsca, gdzie te dane są gromadzone, przechowywane, opracowane, to:
        - Biuro Hotel Malbork**** Centrum Konferencyjne ul. Parkowa 2, 82-200 Malbork
        - Recepcja Hotel Malbork**** Centrum Konferencyjne ul. Parkowa 2, 82-200 Malbork
        - Serwerownia firmy hostingowej
        - Serwerownia firmy dostarczającej oprogramowanie: S4H.
3. Wykaz zbiorów danych osobowych
    - Baza Klientów:
        - Program S4H – forma elektroniczna
        - Program pocztowy – Thunderbird – forma elektroniczna
        - Karta rejestracyjna – forma papierowa
    - Baza kontrahentów:
        - Umowy z kontrahentami – forma papierowa
        - Program S4H – forma elektroniczna
    - Osoby zatrudnione na podstawie umowy cywilno-prawnej i umowy o pracę:
        - Arkusz kalkulacyjny Exel – forma elektroniczna
        - Arkusz tekstu WORD – forma elektroniczna i papierowa
        - Program pocztowy – forma elektroniczna
        - System księgowy
        - System bankowy
        - Inne programy
4. Opis struktury zbiorów danych osobowych:
    - Baza klientów program S4H

- Imię, nazwisko, adres zamieszkania, ulica, numer, kod i miasto, nip, adres e-mail;

- Baza klientów karta rejestracyjna
  - Imię, nazwisko, adres zamieszkania, ulica, numer, kod i miasto, adres e-mail;

5. Sposób przepływu danych:
   - Przepływ danych pomiędzy programami informatycznymi– brak
   - Przepływ danych ze strony www na maila – jednokierunkowy
6. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych
   - Obowiązki Administratora danych osobowych:
     - Wprowadzanie odpowiednich środków technicznych i organizacyjnych, które zapewnią ochronę danych osobowych i jej zgodność z RODO
     - Zastosowanie takich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne w stosunku do każdego konkretnego celu przetwarzania: dotyczy to ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności
     - Analiza ryzyka oraz ocena skutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania
     - Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO
     - Ustalenie celów i zasad przetwarzania danych osobowych
     - Prowadzenie rejestru czynności przetwarzania danych osobowych
     - Wydawanie i anulowanie Upoważnień do przetwarzania danych osobowych
     - Prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych
     - Sprawdzenie podmiotu, któremu administrator powierza przetwarzanie danych osobowych w zakresie gotowości tego podmiotu do zapewnienia odpowiedniej ochrony powierzonych danych osobowych
     - Zgłaszanie naruszeń ochrony danych osobowych do organu nadzorczego oraz zawiadomienie o tym osoby, której dane te dotyczą
     - Wykonanie dodatkowych obowiązków informacyjnych przy zbieraniu danych osobowych
     - Zapewnienie osobom, których dane dotyczą prawa dostępu do danych osobowych – ich sprostowania, usunięcia lub ograniczania przetwarzania

lub prawo wniesienia sprzeciwu wobec przetwarzania a także prawo przenoszenia danych

- Umożliwienie cofnięcia zgody na przetwarzanie danych osobowych w każdej chwili, jeśli taka zgoda uprzednio miała miejsce

- Upoważnienie do przetwarzania danych
  - Podmiot przetwarzający oraz każda osoba działająca z upoważnienia Administratora lub Podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzając je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.
  - Przed nadaniem upoważnienia osoba jest zapoznana z zasadami ochrony danych osobowych zawartymi w Polityce i Instrukcji
  - Osoba zapoznana z zasadami ochrony zobowiązana jest do podpisania Oświadczenia o poufności
  - Administrator danych osobowych nadaje upoważnienie osobie upoważnianej
  - Administrator danych osobowych prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych
- Zabezpieczenie organizacyjne i techniczne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzania danych
  - Zabezpieczenie organizacyjne:
    - ✓ Została opracowana i wdrożona polityka oraz instrukcja
    - ✓ Do przetwarzania danych są dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora
    - ✓ Prowadzony jest rejestr osób upoważnionych do przetwarzania danych
    - ✓ Osoby upoważnione do przetwarzania danych zostały zapoznane z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego
    - ✓ Osoby upoważnione do przetwarzania danych osobowych zostały obowiązane do zachowania ich poufności
    - ✓ Przetwarzanie danych osobowych dokonywane jest w warunkach uniemożliwiających dostęp osób nieupoważnionych
    - ✓ Przebywanie osób nieupoważnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest możliwe tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych
  - Zabezpieczenie fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej

- ✓ Drzwi zamykane na klucz
- ✓ Zamknięte szafy, gdzie przechowywane są dokumenty, które zawierają dane osobowe
- ✓ Dostęp do pomieszczeń objęty jest systemem kontroli dostępu
- ✓ System przeciwpożarowy
- ✓ System monitoringu
- ✓ System antywłamaniowy

➢ Zabezpieczenie sprzętowe infrastruktury informatycznej i telekomunikacyjnej

- ✓ Użyto systemu backupów komputerów, na których są przetwarzane dane osobowe
- ✓ Dostęp do komputera/laptopa z danymi osobowymi jest możliwy tylko po podaniu loginu i hasła
- ✓ Użyto systemu Firewall do ochrony dostępu do sieci komputerowej
- ✓ Zainstalowano program antywirusowy
- ✓ Użyto systemu do ochrony dostępu do sieci komputerowej z zewnątrz

➢ Zabezpieczenie programów przetwarzających dane osobowe

- ✓ Wdrożono system certyfikatu ssl na stronie internetowej www.hotelmalbork.com
- ✓ Dostęp do danych osobowych w systemach informatycznych wymaga podania loginu i hasła
- ✓ Zastosowano wygaszacze ekranu i blokadę ekranu po dłuższej nieaktywności użytkownika

- Procedura postępowania przy naruszeniu bezpieczeństwa danych

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

- ➢ Zniszczenia
- ➢ Utracenia
- ➢ Zmodyfikowania
- ➢ Nieuprawnionego ujawnienia
- ➢ Nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych

KROK 1

Osoba, która ujawniła naruszenie powinna niezwłocznie poinformować o zdarzeniu osobę nadzorującą przetwarzanie danych osobowych (administratora danych)

Krok 2

Osoba nadzorująca przetwarzanie danych osobowych (Administrator):

- Sporządza notatkę z przeprowadzonych oględzin miejsca zdarzenia
- Sporządza kopię obrazu wyświetlonego na ekranie monitora komputera związanego
  z naruszeniem
- Sporządza kopię zapisu rejestrów systemu informatycznego służącego do przetwarzania danych lub zapisów konfiguracji technicznych środków zabezpieczeń systemu
- Odbiera pisemne wyjaśnienia od osoby, która ujawniła naruszenie

Krok 3

- Administrator wpisuje informację o zaistniałym naruszeniu do Rejestru naruszeń ochrony danych osobowych
- Administrator ocenia, czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu
- Jeśli administrator uzna, że zaistniałe naruszenie podlega obowiązkowi zgłoszenia w ciągu 72 godzin od zdarzenia sporządza zgłoszenie do organu nadzorczego oraz zamieszcza informację o naruszeniu na stronie internetowej

7. Zasady udostępniania danych

Udostępnienie Danych osobowych innemu administratorowi oznacza praktyczne przekazanie Danych osobowych.

Skutkiem udostępnienia danych osobowych jest faktyczne przekazanie Danych osobowych w wyniku którego nowy administrator będzie decydował o celach i środkach przetwarzania danych oraz ponosił odpowiedzialność w zakresie przewidzianym dla Administratora.

Udostępnienie danych osobowych wg RODO:

- Wyraźna zgoda osoby, której dane dotyczą – cele marketingowe
- Na podstawie przepisów prawa – sąd, policja, prokuratura
- Innemu administratorowi, jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów

Administrator danych jest zobowiązany do prowadzenia rejestru komu i w jakich okolicznościach udostępnił dane osobowe.

8. Procedura powierzenia danych

- Administrator danych może powierzyć Podmiotowi przetwarzającemu, w drodze umowy przetwarzanie danych
- Podmiotem przetwarzającym może być osoba fizyczna lub prawna organ publiczny, jednostka lub inny podmiot
- Podmiot, który otrzymał w drodze powierzenia Dane osobowe może przetwarzać te dane wyłącznie w celu i zakresie które opisane zostały w umowie z Administratorem
- Administrator ma obowiązek korzystania z usług tylko takich podmiotów przetwarzających które zapewniają odpowiednie środki techniczne i organizacyjne
- Administrator prowadzi rejestr umów powierzenia

Security Policy
CKHM spółka z ograniczoną odpowiedzialnością
operating
Hotel Malbork Conference Center
with its registered office in Malbork
82-200, at ul. Parkowa 2

The Personal Data Protection Security Policy at CKHM spółka z ograniczoną odpowiedzialnością with its registered office in Malbork, operating Hotel Malbork**** Conference Center, hereinafter referred to as the **Security Policy**, sets out the procedure in the event of personal data processing and data security breaches. It is intended for persons working on the processing of personal data at CKHM spółka z ograniczoną odpowiedzialnością operating Hotel Malbork**** Conference Center with its registered office in Malbork 82-200 at ul. Parkowa 2.

Definitions

Whenever reference is made in this document to:

- **Security Policy** – shall mean the security policy regarding the protection of personal data at CKHM spółka z ograniczoną odpowiedzialnością with its registered office in Malbork (82-200), ul. Parkowa 2, entered into the Register of Entrepreneurs of the National Court Register kept by the District Court Gdańsk-Północ in Gdańsk, VII Commercial Division of the National Court Register under KRS number 0001108048, REGON: 528740774, NIP: 5792295679, operating Hotel Malbork**** Conference Center in Malbork.
- **GDPR** – shall mean 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.
- **Controller** – shall mean CKHM spółka z ograniczoną odpowiedzialnością with its registered office in Malbork (82-200), ul. Parkowa 2, entered into the Register of Entrepreneurs of the National Court Register kept by the District Court Gdańsk-Północ in Gdańsk, VII Commercial Division of the National Court Register under KRS number 0001108048, REGON: 528740774, NIP: 5792295679, operating Hotel Malbork**** Conference Center with its registered office in Malbork 82-200 at ul. Parkowa 2.
- **Processor** – shall mean a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.
- **Third party** – shall mean a natural or legal person, public authority, agency, or body other than the data subject, Controller, Processor, and persons who, under the direct authority of the Controller or Processor, are authorized to process personal data.
- **Recipient** – shall mean a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- **Personal data** – shall mean any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

- **Data processing** – shall mean any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- **Filing system (Data Set)** – shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis.
- **Consent of the data subject** – shall mean any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **IT system** – shall mean a set of interconnected equipment, programs, information processing procedures, and software tools used for data processing.
- **Data security in an IT system** – shall mean the implementation and operation of appropriate technical and organizational measures to ensure the protection of data against unauthorized processing.
- **IT system management instruction** – shall mean the Instruction for Managing the IT System used for processing personal data at CKHM spółka z ograniczoną odpowiedzialnością operating Hotel Malbork**** Conference Center.

Personal Data Processing Areas

Areas of personal data processing – places where these data are collected, stored, and processed:

- **Office**: Hotel Malbork**** Conference Center, ul. Parkowa 2, 82-200 Malbork
- **Reception**: Hotel Malbork**** Conference Center, ul. Parkowa 2, 82-200 Malbork
- **Server room** of the hosting company
- **Server room** of the software provider: S4H

List of Personal Data Sets

- **Customer Database:**
  - S4H software – electronic form
  - Email client – Thunderbird – electronic form
  - Registration card – paper form
- **Contractor Database:**
  - Contracts with contractors – paper form
  - S4H software – electronic form
- **Persons employed under civil law contracts and employment contracts:**
  - Excel spreadsheet – electronic form
  - Word document – electronic and paper form
  - Email client – electronic form
  - Accounting system
  - Banking system
  - Other software

Description of Data Set Structure

- **Customer database (S4H program):**
  - First name, last name, residential address, street, number, postal code and city, NIP (Tax Identification Number), email address;
- **Customer database (registration card):**
  - First name, last name, residential address, street, number, postal code and city, email address;

Data Flow

- **Data flow between IT programs:** none
- **Data flow from the website to email:** one-way

Technical and Organizational Measures to Ensure Confidentiality, Integrity, and Accountability

Duties of the Personal Data Controller:

- Implementing appropriate technical and organizational measures to ensure personal data protection and compliance with GDPR.
- Applying technical and organizational measures to ensure that, by default, only personal data necessary for each specific purpose of processing are processed (applies to the amount of data collected, the extent of processing, storage period, and accessibility).
- Conducting risk analysis and impact assessments of planned processing operations before initiating data processing.
- Organizing security and protection of personal data in accordance with GDPR requirements.
- Establishing the purposes and rules of personal data processing.
- Maintaining a register of processing activities.
- Issuing and revoking Authorizations to process personal data.
- Maintaining a register of persons authorized to process personal data.
- Verifying the readiness of any entity to which the Controller entrusts personal data processing to ensure appropriate protection of the entrusted data.
- Reporting personal data breaches to the supervisory authority and notifying affected data subjects.
- Fulfilling additional information obligations when collecting personal data.
- Ensuring data subjects can exercise their rights to access, rectify, erase, or restrict processing, object to processing, and data portability.
- Enabling withdrawal of consent for personal data processing at any time, if consent was previously granted.

Authorization to Process Data:

- The Processor and any person acting under the authority of the Controller or Processor with access to personal data process them strictly on instructions from the Controller, unless required to do so by Union or Member State law.
- Prior to authorization, the individual is briefed on the personal data protection rules contained in the Policy and Instruction.
- Persons briefed on protection rules must sign a Confidentiality Declaration.
- The Personal Data Controller issues the authorization to the designated person.
- The Personal Data Controller maintains a register of persons authorized to process personal data.

Organizational and Technical Security Measures:

- **Organizational Security:**
  - Policy and instruction have been developed and implemented.
  - Only individuals authorized by the Controller are permitted to process data.
  - A register of authorized personnel is maintained.
  - Authorized personnel have been trained in personal data protection regulations and IT security procedures.
  - Authorized personnel are bound by confidentiality obligations.
  - Processing takes place under conditions preventing unauthorized access.
  - Unauthorized individuals may only enter rooms where personal data are processed in the presence of authorized personnel and under secure conditions.
- **Physical Security of Premises:**
  - Lockable doors.
  - Locked cabinets for storing physical documents containing personal data.
  - Access control system for room access.
  - Fire suppression system.
  - Alarm/monitoring system.
  - Anti-burglar system.
- **Hardware and IT Security:**
  - Computer backup system for devices used to process data.
  - Access to computers/laptops with personal data requires a login and password.
  - Firewall system used to protect computer network access.
  - Antivirus software installed.
  - External network access protection system.
- **Software Security:**
  - SSL certificate implemented on the website (www.hotelmalbork.com).
  - Access to personal data in IT systems requires login credentials.
  - Screen savers and automatic screen lock after user inactivity enabled.

Procedure in Case of a Security Breach

A personal data breach means a breach of security leading to the accidental or unlawful:

- Destruction
- Loss
- Alteration
- Unauthorized disclosure
- Unauthorized access to personal data transmitted, stored, or otherwise processed

STEP 1:

The person who discovers a breach must immediately inform the supervisor overseeing data processing (Data Controller).

STEP 2:

The supervisor overseeing data processing (Controller):

- Drafts a note from the site inspection.
- Makes a copy of the screen display related to the breach.
- Makes a copy of IT system log entries or technical security configurations.
- Obtains written explanations from the person who discovered the breach.

STEP 3:

- The Controller logs the breach details in the Personal Data Breach Register.

- The Controller assesses whether the breach must be reported to the supervisory authority.
- If subject to mandatory notification, the Controller prepares a report to the supervisory authority within 72 hours of discovery and publishes information about the breach on the website.

Rules for Sharing Data

Sharing personal data with another controller means the practical transfer of data, resulting in a new controller who decides the purposes and means of processing and assumes liability.
Under GDPR, sharing data requires:

- Explicit consent from the data subject (for marketing purposes).
- A legal basis (e.g., courts, police, prosecutor's office).
- Legitimate interest of another controller (where applicable).

The Controller must maintain a register of to whom and under what circumstances data were shared.

Data Entrustment Procedure

- The Controller may entrust processing to a Processor via a written contract.
- A Processor can be a natural or legal person, public authority, agency, or other body.
- The Processor may process entrusted personal data solely for the purposes and scope outlined in the agreement.
- The Controller is obligated to use only Processors providing sufficient technical and organizational measures.
- The Controller maintains a register of data entrustment agreements.