HOTEL MALBORK**** CENTRUM KONFERENCYJNE
POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH (RODO)

*CKHM spółki z ograniczoną odpowiedzialnością prowadzącej Hotel Malbork**** Centrum Konferencyjne z siedzibą w Malborku (82-200), przy ul. Parkowej 2*

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w CKHM spółce z ograniczoną odpowiedzialnością z siedzibą w Malborku, prowadzącej Hotel Malbork**** Centrum Konferencyjne (dalej także Hotel), zwana dalej Polityką Bezpieczeństwa, określa zasady i sposób postępowania przy przetwarzaniu danych osobowych oraz w sytuacji naruszenia ochrony tych danych. Dokument jest przeznaczony dla wszystkich osób przetwarzających dane osobowe w imieniu Administratora.

1. Definicje

- **Polityka Bezpieczeństwa –** niniejsza polityka 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 KRS prowadzonego przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VII Wydział Gospodarczy KRS pod numerem KRS: 0001108048, REGON: 528740774, NIP: 5792295679, prowadzącej Hotel Malbork**** Centrum Konferencyjne w Malborku.
- **RODO –** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
- **Administrator –** CKHM spółka z ograniczoną odpowiedzialnością z siedzibą w Malborku (82-200), ul. Parkowa 2, KRS: 0001108048, REGON: 528740774, NIP: 5792295679, kontakt: recepcja@hotelmalbork.com.
- **Inspektor Ochrony Danych (IOD) –** osoba wyznaczona przez Administratora do nadzorowania przestrzegania przepisów o ochronie danych osobowych, z którą można skontaktować się pod adresem e-mail: a.nadolski@prino-plast.pl.
- **Podmiot przetwarzający (Procesor) –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora na podstawie umowy powierzenia (art. 28 RODO).
- **Strona trzecia –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot inny niż osoba, której dane dotyczą, Administrator, Podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub Podmiotu przetwarzającego mogą przetwarzać dane osobowe.
- **Odbiorca danych –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (z wyłączeniem organów publicznych otrzymujących dane w ramach konkretnego postępowania zgodnie z prawem).
- **Dane osobowe –** wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (Gościu, Użytkowniku, Pracowniku, Kontrahencie).
- **Przetwarzanie danych –** operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany (zbieranie, utrwalanie, organizowanie, przechowywanie, modyfikowanie, przeglądanie, wykorzystywanie, przesyłanie, usuwanie lub niszczenie).
- **Zbiór danych –** uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów.
- **Zgoda osoby, której dane dotyczą –** dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przyzwalające na przetwarzanie danych osobowych (np. zgoda marketingowa lub zgoda na pliki Cookies w banerze na stronie www.hotelmalbork.com).

- **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Instrukcja zarządzania systemem informatycznym** – Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych obowiązująca u Administratora.

2. Obszary przetwarzania danych osobowych

Obszary przetwarzania danych osobowych (miejsca fizyczne oraz środowiska chmurowe/serwerowe, gdzie dane są gromadzone, przechowywane i opracowywane):

- Biuro Administratora: Hotel Malbork**** Centrum Konferencyjne, ul. Parkowa 2, 82-200 Malbork;
- Recepcja Hotel Malbork**** Centrum Konferencyjne, ul. Parkowa 2, 82-200 Malbork;
- Pomieszczenie techniczne / rejestrator monitoringu wizyjnego (CCTV) na terenie siedziby Administratora przy ul. Parkowej 2 w Malborku;
- Serwerownia firmy hostingowej obsługującej stronę internetową www.hotelmalbork.com oraz pocztę elektroniczną Administratora;
- Serwerownia / infrastruktura dostawcy oprogramowania hotelowego (PMS): S4H;
- Infrastruktura chmurowa dostawcy silnika rezerwacyjnego i CRM: Profitroom S.A.;
- Infrastruktura chmurowa dostawcy oprogramowania biurowego i poczty elektronicznej: Microsoft (Microsoft 365 / Outlook).

3. Wykaz zbiorów danych osobowych i okresy ich przechowywania (retencji)

3.1. Baza Gości i Klientów (usługi hotelarskie, gastronomiczne, SPA, konferencyjne)

- **Narzędzia i forma:** System hotelowy S4H (elektroniczna), silnik rezerwacyjny i CRM Profitroom (elektroniczna), klient pocztowy Microsoft Outlook (elektroniczna), komunikatory WhatsApp / Messenger (elektroniczna), Karta rejestracyjna Gościa (papierowa), dokumentacja księgowo-podatkowa (elektroniczna i papierowa).
- **Okres przechowywania:** przez czas trwania umowy, a po jej zakończeniu przez okres przedawnienia roszczeń cywilnoprawnych; dokumentacja księgowa i podatkowa – przez 5 lat licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku wynikającego z dokumentu księgowo rachunkowego wystawionego w związku z realizacją danej mowy na usługi.

3.2. Baza Marketingowa i Ofertowanie Pobytowe

- **Narzędzia i forma:** System CRM / Marketing Automation Profitroom oraz klient pocztowy Microsoft Outlook (forma elektroniczna).
- **Okres przechowywania:** do momentu wycofania zgody przez Gościa lub wniesienia skutecznego sprzeciwu wobec przetwarzania danych w celach marketingowych.

3.3. Zbiór Monitoringu Wizyjnego (CCTV)

- **Narzędzia i forma:** Rejestrator wizyjny obejmujący strefy ogólnodostępne Hotelu (recepcja, korytarze, parking, wejścia do budynku).
- **Okres przechowywania:** maksymalnie do 30 dni od dnia nagrania (chyba że nagranie stanowi dowód w postępowaniu – wówczas do czasu prawomocnego zakończenia postępowania).

3.4. Użytkownicy Strony Internetowej www.hotelmalbork.com oraz Mediów Społecznościowych

- **Narzędzia i forma:** Logi serwera, narzędzie zarządzania zgodami Cookies, narzędzia analityczne/marketingowe (Google, Meta Platforms), profile Facebook i Instagram.

3.5. Baza Kontrahentów

- **Narzędzia i forma:** Umowy z kontrahentami (forma papierowa), system S4H oraz system księgowy (forma elektroniczna).

3.6. Baza osób zatrudnionych przez Administratora na podstawie umowy o pracę oraz umów cywilnoprawnych

- **Narzędzia i forma:** Arkusze kalkulacyjne Microsoft Excel (elektroniczna), dokumenty Microsoft Word (elektroniczna i papierowa), poczta Microsoft Outlook (elektroniczna), system kadrowo-księgowy, system bankowy, teczki osobowe (papierowa).

4. Opis struktury zbiorów danych osobowych

- **Baza Gości (program S4H / Profitroom / Karta rejestracyjna):** imię, nazwisko, adres zamieszkania (ulica, numer, kod pocztowy, miejscowość), numer telefonu, adres e-mail, numer dokumentu tożsamości (w celu weryfikacji tożsamości przy zameldowaniu), dane dotyczące pobytu (daty, historia rezerwacji, preferencje), dane do faktury (nazwa firmy, NIP), dane płatnicze.
- **Baza zapytań i komunikacji (Microsoft Outlook, formularz www, WhatsApp, Messenger):** imię, nazwisko, adres e-mail, numer telefonu, nazwa profilu społecznościowego (Facebook, Instagram, Messenger, WhatsApp) oraz treść korespondencji.
- **Monitoring wizyjny (CCTV):** wizerunek osób przebywających w strefach ogólnodostępnych Hotelu, numery rejestracyjne pojazdów na parkingu hotelowym.
- **Logi serwera i pliki Cookies:** adres IP, czas zapytania, informacje o przeglądarce i systemie operacyjnym, identyfikatory plików Cookies (niezbędne, analityczne, marketingowe).

5. Sposób przepływu danych

- Przepływ danych pomiędzy lokalnymi programami informatycznymi – brak automatycznej synchronizacji lokalnej (z wyłączeniem integracji silnika rezerwacyjnego Profitroom z systemem hotelowym S4H).
- Przepływ danych ze strony internetowej www.hotelmalbork.com (formularz kontaktowy) – jednokierunkowy, szyfrowany (SSL), kierowany na skrzynkę e-mail recepcja@hotelmalbork.com obsługiwaną w programie Microsoft Outlook.
- Przepływ danych z rezerwacji online (Booking Engine Profitroom) – szyfrowany transfer pomiędzy platformą Profitroom a recepcją Hotelu.
- Przepływ danych z komunikatorów i mediów społecznościowych (WhatsApp, Messenger, Facebook, Instagram) – dwukierunkowy w ramach bieżącej obsługi zapytań Gości przez upoważnionych pracowników recepcji i marketingu.

6. Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych

6.1. Obowiązki Administratora Danych Osobowych (przy wsparciu IOD)

- Wdrażanie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych oraz zgodność z art. 5 i art. 32 RODO;
- Stosowanie zasady minimalizacji danych i ochrony danych w fazie projektowania oraz domyślnej ochrony danych (Privacy by Design & Privacy by Default);

- Przeprowadzanie analizy ryzyka oraz oceny skutków dla ochrony danych (DPIA), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
- Prowadzenie Rejestru Czynności Przetwarzania Danych Osobowych (art. 30 RODO);
- Wydawanie i anulowanie pisemnych Upoważnień do przetwarzania danych osobowych oraz prowadzenie Ewidencji osób upoważnionych;
- Weryfikacja podmiotów przetwarzających (procesorów) przed powierzeniem im danych i zawieranie umów powierzenia (art. 28 RODO);
- Realizacja obowiązku informacyjnego wobec Gości, Użytkowników, Pracowników i Kontrahentów (art. 13 i 14 RODO) za pośrednictwem klauzul informacyjnych oraz Polityki Prywatności na stronie www.hotelmalbork.com;
- Zapewnienie osobom, których dane dotyczą, realizacji ich praw (dostępu, sprostowania, usunięcia, ograniczenia, przenoszenia, sprzeciwu oraz wycofania zgody w dowolnym momencie – obsługa zgłoszeń pod adresem recepcja@hotelmalbork.com we współpracy z IOD);
- Zgłaszanie naruszeń ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych (PUODO) oraz zawiadamianie osób, których dane dotyczą, w przypadkach wymaganych prawem.

6.2. Upoważnienie do przetwarzania danych

- Każda osoba działająca z upoważnienia Administratora (pracownik, współpracownik) może przetwarzać dane osobowe wyłącznie na wyraźne polecenie Administratora.
- Przed dopuszczeniem do pracy z danymi osoba jest szkolona i zapoznawana przez Administratora z zasadami zawartymi w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.
- Osoba upoważniona przez Administratora do przetwarzania danych podpisuje pisemne Oświadczenie o zachowaniu poufności (obowiązujące również po ustaniu zatrudnienia).
- Administrator nadaje pisemne upoważnienie i wpisuje je do Ewidencji osób upoważnionych.

6.3. Zabezpieczenia organizacyjne, fizyczne, sprzętowe i programowe stosowane przez Administratora

- **Zabezpieczenia organizacyjne:**
  - Wdrożona Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym oraz Polityka Prywatności i Plików Cookies;
  - Dopuszczanie do przetwarzania danych wyłącznie osób posiadających imienne upoważnienie i wpisanych do ewidencji;
  - Stosowanie zasady „czystego biurka" oraz „czystego ekranu";
  - Przy wysyłce korespondencji grupowej/marketingowej za pośrednictwem programu Microsoft Outlook obowiązek stosowania pola „UDW" (Ukryte do wiadomości / BCC) lub dedykowanych narzędzi mailingowych (Profitroom) w celu uniemożliwienia ujawnienia adresów e-mail odbiorców między sobą;
  - Przebywanie osób nieupoważnionych w pomieszczeniach, gdzie przetwarzane są dane (biuro, zaplecze recepcji), dozwolone jest wyłącznie w obecności osoby upoważnionej.
- **Zabezpieczenia fizyczne pomieszczeń:**
  - Drzwi do pomieszczeń biurowych i zaplecza recepcji zamykane na klucz;
  - Szafy zamykane na klucz, w których przechowywane są dokumenty papierowe (karty rejestracyjne, umowy, teczki osobowe);
  - System kontroli dostępu do stref zamkniętych;
  - System przeciwpożarowy, system alarmowy oraz system antywłamaniowy;

  - Monitoring wizyjny (CCTV) obejmujący wejścia, recepcję, korytarze oraz parking.
- **Zabezpieczenia sprzętowe i infrastrukturalne:**
  - Regularne wykonywanie kopii zapasowych (backupów) baz danych oraz stacji roboczych;
  - Dostęp do komputerów, laptopów i urządzeń służbowych zabezpieczony indywidualnym loginem i silnym hasłem;
  - Zabezpieczenie sieci lokalnej za pomocą zapory sieciowej (Firewall) oraz systemów ochrony przed nieuprawnionym dostępem z zewnątrz;
  - Zainstalowane i na bieżąco aktualizowane oprogramowanie antywirusowe.
- **Zabezpieczenia programowe i telekomunikacyjne:**
  - Certyfikat SSL (szyfrowanie HTTPS) wdrożony na stronie internetowej www.hotelmalbork.com;
  - Indywidualne konta użytkowników z uwierzytelnianiem (login i hasło) w systemach S4H, Profitroom, Microsoft Outlook oraz systemach księgowo-bankowych;
  - Automatyczna blokada ekranu (wygaszacz zabezpieczony hasłem) po krótkim okresie nieaktywności użytkownika;
  - Szyfrowanie urządzeń mobilnych / służbowych wykorzystywanych do obsługi komunikatorów (WhatsApp, Messenger).

7. Procedura postępowania przy naruszeniu ochrony danych osobowych

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

- **KROK 1 – Zgłoszenie wewnętrzne:** Osoba, która ujawniła lub podejrzewa naruszenie, niezwłocznie informuje Administratora oraz Inspektora Ochrony Danych (e-mail: a.nadolski@prino-plast.pl), powstrzymując się od działań mogących zatrzeć ślady zdarzenia.
- **KROK 2 – Zabezpieczenie dowodów i analiza zdarzenia:** Administrator we współpracy z IOD sporządza notatkę z oględzin miejsca zdarzenia, zabezpiecza zrzuty ekranu, logi systemowe oraz zapisy konfiguracji zabezpieczeń, a także odbiera pisemne wyjaśnienia od osoby, która ujawniła naruszenie.
- **KROK 3 – Ocena ryzyka, Rejestr Naruszeń i zgłoszenie do PUODO (art. 33 i 34 RODO):** Administrator wpisuje zdarzenie do Rejestru Naruszeń Ochrony Danych Osobowych i wraz z IOD ocenia ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli naruszenie może skutkować takim ryzykiem, Administrator zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych (PUODO) bez zbędnej zwłoki – nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. Jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator niezwłocznie zawiadamia o nim również osoby, których dane dotyczą.

8. Powierzenie przetwarzania, udostępnianie, współadministrowanie oraz transfer poza EOG

8.1. Powierzenie przetwarzania danych (art. 28 RODO)

Administrator powierza przetwarzanie danych osobowych wyłącznie podmiotom zapewniającym wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, na podstawie pisemnych lub elektronicznych umów powierzenia (DPA). Do głównych procesorów należą: Profitroom S.A., dostawca systemu S4H, firma hostingowa, Microsoft (Microsoft 365 / Outlook), biuro rachunkowe, kancelarie prawne oraz firmy ochroniarskie/IT. Administrator prowadzi Rejestr Umów Powierzenia.

8.2. Udostępnianie danych i Współadministrowanie

- **Udostępnianie danych:** następuje wyłącznie na podstawie przepisów prawa (np. Policja, sądy, organy skarbowe) lub w celu realizacji usług (operatorzy płatności, banki, portale rezerwacyjne OTA). Administrator ewidencjonuje przypadki udostępniania danych.
- **Współadministrowanie (art. 26 RODO):** Administrator oraz Meta Platforms Ireland Limited pełnią funkcję wspólnych administratorów danych w zakresie statystyk stron (Page Insights) na platformach Facebook i Instagram.

8.3. Przekazywanie danych poza Europejski Obszar Gospodarczy (EOG)

W związku z korzystaniem z narzędzi dostawców takich jak Microsoft, Meta Platforms (Facebook, Instagram, Messenger, WhatsApp) oraz Google, dane mogą być przekazywane poza EOG (m.in. do USA). Transfer ten odbywa się wyłącznie w oparciu o decyzje Komisji Europejskiej stwierdzające odpowiedni stopień ochrony (EU-US Data Privacy Framework) lub standardowe klauzule umowne (SCC).

HOTEL MALBORK**** CONFERENCE CENTRE

PERSONAL DATA PROTECTION SECURITY POLICY (GDPR)

CKHM spółka z ograniczoną odpowiedzialnością, operating Hotel Malbork** Conference Centre, with its registered office in Malbork (82-200) at ul. Parkowa 2.**

The data protection security policy at CKHM spółka z ograniczoną odpowiedzialnością, with its registered office in Malbork, operating Hotel Malbork**** Conference Centre (hereinafter also referred to as the Hotel), hereinafter referred to as the Security Policy, defines the principles and procedures for processing personal data and for handling personal data breaches. This document is intended for all persons processing personal data on behalf of the Controller.

1. Definitions

- Security Policy: This personal data protection security policy of 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 maintained by the District Court Gdańsk-Północ in Gdańsk, 7th Commercial Division of the National Court Register under KRS number: 0001108048, REGON: 528740774, NIP: 5792295679, operating Hotel Malbork**** Conference Centre in Malbork.
- 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.
- Controller: CKHM spółka z ograniczoną odpowiedzialnością with its registered office in Malbork (82-200), ul. Parkowa 2, KRS: 0001108048, REGON: 528740774, NIP: 5792295679, contact: recepcja@hotelmalbork.com.
- Data Protection Officer (DPO): A person designated by the Controller to supervise compliance with personal data protection regulations, who can be contacted via email: a.nadolski@prino-plast.pl.
- Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller based on a data processing agreement (Article 28 GDPR).
- Third Party: 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 authorised to process personal data.
- Recipient: A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not (excluding public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law).
- Personal Data: Any information relating to an identified or identifiable natural person (Guest, User, Employee, Contractor).
- Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (such as collection, recording, organisation, 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: Any structured set of personal data which are accessible according to specific criteria.

- Data Subject's Consent: 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 (e.g., marketing consent or Cookie consent via the banner at www.hotelmalbork.com).
- IT System: A set of cooperating devices, programs, information processing procedures, and software tools used for data processing.
- IT System Management Instruction: The instruction for managing the IT system used for processing personal data in force at the Controller's organization.

2. Areas of Personal Data Processing

Areas of personal data processing (physical locations and cloud/server environments where data is collected, stored, and processed):

- Controller's Office: Hotel Malbork**** Conference Centre, ul. Parkowa 2, 82-200 Malbork;
- Reception: Hotel Malbork**** Conference Centre, ul. Parkowa 2, 82-200 Malbork;
- Technical Room / CCTV Surveillance Recorder: located on the premises of the Controller at ul. Parkowa 2 in Malbork;
- Server Room of the hosting company: maintaining the website www.hotelmalbork.com and the Controller's email;
- Server Room / Infrastructure of the Hotel Property Management System (PMS) provider: S4H;
- Cloud Infrastructure of the Booking Engine and CRM provider: Profitroom S.A.;
- Cloud Infrastructure of the office software and email provider: Microsoft (Microsoft 365 / Outlook).

3. Register of Personal Data Sets and Retention Periods

3.1. Guest and Customer Database

(hotel, catering, SPA, and conference services)

- Tools and Form: S4H hotel system (electronic), Profitroom booking engine and CRM (electronic), Microsoft Outlook email client (electronic), WhatsApp / Messenger communication apps (electronic), Guest Registration Card (paper), accounting and tax documentation (electronic and paper).
- Retention Period: For the duration of the agreement, and after its termination, for the period of limitation of civil law claims; accounting and tax documentation – for 5 years starting from the end of the calendar year in which the tax payment deadline expired regarding the accounting document issued in connection with the performance of a given service agreement.

3.2. Marketing and Stay Quotations Database

- Tools and Form: Profitroom CRM / Marketing Automation system and Microsoft Outlook email client (electronic form).
- Retention Period: Until the Guest withdraws consent or raises an effective objection to the processing of data for marketing purposes.

3.3. Video Surveillance (CCTV) Dataset

- Tools and Form: Video recorder covering public areas of the Hotel (reception, corridors, parking lot, building entrances).
- Retention Period: Maximum up to 30 days from the date of recording (unless the recording constitutes evidence in a proceeding – then until the final conclusion of the proceeding).

3.4. Users of the Website www.hotelmalbork.com and Social Media

- Tools and Form: Server logs, Cookie consent management tool, analytical/marketing tools (Google, Meta Platforms), Facebook and Instagram profiles.

3.5. Contractors Database

- Tools and Form: Contractor agreements (paper form), S4H system and accounting system (electronic form).

3.6. Database of Persons Employed by the Controller under Employment Contracts and Civil Law Contracts

- Tools and Form: Microsoft Excel spreadsheets (electronic), Microsoft Word documents (electronic and paper), Microsoft Outlook mail (electronic), HR and payroll system, banking system, personnel files (paper).

4. Description of Personal Data Structure

- Guest Database (S4H program / Profitroom / Registration Card): first name, last name, residential address (street, number, postal code, city), phone number, email address, ID document number (for verification purposes upon check-in), stay details (dates, reservation history, preferences), invoice details (company name, NIP / tax ID), payment data.
- Inquiries and Communication Database (Microsoft Outlook, website form, WhatsApp, Messenger): first name, last name, email address, phone number, social media profile name (Facebook, Instagram, Messenger, WhatsApp) and correspondence content.
- Video Surveillance (CCTV): image of persons staying in public areas of the Hotel, vehicle registration numbers in the hotel parking lot.
- Server Logs and Cookies: IP address, query time, browser and operating system information, Cookie identifiers (necessary, analytical, marketing).

5. Data Flow

- Data flow between local IT programs: No automatic local synchronization (excluding the integration of the Profitroom booking engine with the S4H hotel system).
- Data flow from the website www.hotelmalbork.com (contact form): Unidirectional, encrypted (SSL), directed to recepcja@hotelmalbork.com handled via Microsoft Outlook.
- Data flow from online reservations (Profitroom Booking Engine): Encrypted transfer between the Profitroom platform and the Hotel reception.
- Data flow from messengers and social media (WhatsApp, Messenger, Facebook, Instagram): Bidirectional within the ongoing handling of Guest inquiries by authorized reception and marketing staff.

6. Technical and Organizational Measures Ensuring Data Security

6.1. Obligations of the Personal Data Controller (with DPO Support)

- Implementation of appropriate technical and organizational measures to ensure data protection and compliance with Article 5 and Article 32 of the GDPR;
- Application of data minimisation, privacy by design, and privacy by default principles;
- Conducting risk analysis and Data Protection Impact Assessments (DPIA) if a given type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
- Maintaining the Register of Personal Data Processing Activities (Article 30 GDPR);
- Issuing and revoking written Authorizations to process personal data and maintaining the Register of Authorized Persons;
- Verifying processors before entrusting them with data and concluding data processing agreements (Article 28 GDPR);
- Fulfillment of the information obligation towards Guests, Users, Employees, and Contractors (Articles 13 and 14 GDPR) via information clauses and the Privacy Policy at www.hotelmalbork.com;
- Ensuring that data subjects can exercise their rights (access, rectification, erasure, restriction, portability, objection, and withdrawal of consent at any time – handling requests at recepcja@hotelmalbork.com in cooperation with the DPO);
- Reporting personal data breaches to the President of the Personal Data Protection Office (UODO) and notifying data subjects in cases required by law.

6.2. Authorization to Process Data

- Each person acting under the authority of the Controller (employee, collaborator) may process personal data solely upon the explicit instruction of the Controller.
- Before being allowed to work with data, the person is trained and familiarized by the Controller with the rules contained in the Security Policy and the IT System Management Instruction.
- An individual authorized by the Controller to process data signs a written Confidentiality Statement (which remains in force even after the termination of employment).
- The Controller grants a written authorization and enters it into the Register of Authorized Persons.

6.3. Organizational, Physical, Hardware, and Software Safeguards Applied by the Controller

- Organizational Safeguards:
    - Implemented Security Policy, IT System Management Instruction, and Privacy and Cookies Policy;
    - Permitting data processing exclusively by persons holding individual authorizations and entered into the register;
    - Application of the "clean desk" and "clean screen" principles;
    - When sending group/marketing correspondence via Microsoft Outlook, the obligation to use the "BCC" (Blind Carbon Copy) field or dedicated mailing tools (profitroom) to prevent recipients' email addresses from being disclosed to each other;
    - Unauthorized persons are permitted in rooms where data is processed (office, reception back office) solely in the presence of an authorized person.
- Physical Room Safeguards:

  - Office and reception back-office doors locked with a key;
  - Lockable cabinets where paper documents are stored (registration cards, agreements, personnel files);
  - Access control system for restricted zones;
  - Fire protection system, alarm system, and anti-burglary system;
  - Video surveillance (CCTV) covering entrances, reception, corridors, and parking.
- Hardware and Infrastructure Safeguards:
  - Regular backups of databases and workstations;
  - Access to corporate computers, laptops, and devices secured with an individual login and strong password;
  - Securing the local network using a Firewall and intrusion prevention systems against unauthorized external access;
  - Installed and regularly updated antivirus software.
- Software and Telecommunications Safeguards:
  - SSL certificate (HTTPS encryption) implemented on www.hotelmalbork.com;
  - Individual user accounts with authentication (login and password) in S4H, Profitroom, Microsoft Outlook, and accounting/banking systems;
  - Automatic screen lock (password-protected screensaver) after a short period of user inactivity;
  - Encryption of mobile/corporate devices used to handle messengers (WhatsApp, Messenger).

7. Personal Data Breach Procedure

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- STEP 1 – Internal Reporting: A person who has discovered or suspects a breach immediately informs the Controller and the Data Protection Officer (email: a.nadolski@prino-plast.pl), refraining from actions that could obliterate the traces of the event.
- STEP 2 – Evidence Securing and Event Analysis: The Controller, in cooperation with the DPO, draws up a note from the site inspection of the incident, secures screen shots, system logs, and security configuration records, and collects written explanations from the person who discovered the breach.
- STEP 3 – Risk Assessment, Breach Register, and Notification to UODO (Articles 33 and 34 GDPR): The Controller enters the incident into the Personal Data Breach Register and, together with the DPO, assesses the risk to the rights and freedoms of natural persons. If the breach is likely to result in such risk, the Controller notifies the President of the Personal Data Protection Office (UODO) without undue delay and, where feasible, not later than 72 hours after having become aware of it. If the breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall also communicate the breach to the data subjects without undue delay.

8. Entrusting Processing, Sharing, Joint Controllership, and Transfers Outside the EEA

8.1. Entrusting Data Processing (Article 28 GDPR)

The Controller entrusts the processing of personal data exclusively to entities providing sufficient guarantees to implement appropriate technical and organizational measures, based on written or electronic data processing agreements (DPA). The main processors include: Profitroom S.A., the S4H system provider, hosting company, Microsoft (Microsoft 365 / Outlook), accounting office, law firms, and security/IT companies. The Controller maintains a Register of Processing Agreements.

8.2. Data Sharing and Joint Controllership

- Data Sharing: Occurs solely on the basis of legal provisions (e.g., Police, courts, tax authorities) or for the execution of services (payment operators, banks, OTA reservation portals). The Controller logs instances of data sharing.
- Joint Controllership (Article 26 GDPR): The Controller and Meta Platforms Ireland Limited act as joint data controllers regarding page insights on Facebook and Instagram platforms.

8.3. Transfer of Data Outside the European Economic Area (EEA)

Due to the use of tools from providers such as Microsoft, Meta Platforms (Facebook, Instagram, Messenger, WhatsApp), and Google, data may be transferred outside the EEA (including to the USA). Such transfers take place solely based on European Commission adequacy decisions (EU-US Data Privacy Framework) or Standard Contractual Clauses (SCC).