

GROUP DATA PROTECTION POLICY

Summary

This Group Data Protection Policy (“**Data Protection Policy**”) stipulates the rules for personal data protection in the CPI PROPERTY GROUP (“**CPIPG**”) and its affiliated companies (“**CPIPG companies**”). It provides for the rules of personal data protection, including related obligations of the CPIPG companies. The Data Protection Policy reflects the data privacy rules required by the GDPR and other Member States’ national data privacy legislation.

The CPIPG companies take personal data protection seriously and handle the personal data with sufficient carefulness and responsibility when performing their business activities. A personal data breach may result in serious legal and economic consequences for the CPIPG companies, their employees and data subjects. It may also cause damage to the CPIPG companies’ reputation. Through the implementation of the Data Protection Policy across the CPIPG companies, the risks of, and arising from, breaching data protection will be minimised.

Applicability

This Data Protection Policy is binding for the CPIPG companies and their employees. It relates to all personal data

processing to which the GDPR and the Member States’ national legislation apply.

1. Procedure and Competencies

The following articles describe the procedures followed by the CPIPG companies when processing the personal data.

Furthermore, they provide a brief description of the split of the competencies and key roles in the CPIPG companies in the area of personal data processing.

1.1 General Obligation

The CPIPG companies have taken and shall continue to take appropriate technical and organisational measures in order to ensure the protection of the personal data against misuse, loss and damage, and to treat them in accordance with the GDPR and the Member States’ national legislation in the area of data privacy. The data protection applies to the processing of the personal data of the CPIPG companies’ partners, employees, their family members, job applicants, customers and other individuals whose personal data are processed by the CPIPG companies.

1.2 Basic Principles of Personal Data Protection

The CPIPG companies respect the basic principles stipulated by the GDPR in processing the personal data. The respective basic principles are listed below:

- Lawfulness principle – at least one lawful basis has to be determined prior to processing the personal data;
- Principle of limitation by purpose – process the personal data only for pre-defined purposes;
- Data minimisation principle – processing of only necessary, relevant and adequate personal data for any legitimate purpose;
- Correctness and transparency principle – open and transparent processing to the data subjects;
- Integrity and confidentiality principle, application of the “need to know” principle – implementation of necessary organisational and technical measures in order to ensure the restriction of access to the personal data to prevent an unauthorised or unlawful processing;
- Accuracy principle – processing of accurate and up-to-date personal data;
- Controlled change management regime – a change of the current processing system to a new method is a subject to the DPO’s or controller’s consideration and a potential subsequent preparation of the Data Privacy Impact Assessment;
- Definition of roles participating in the personal data protection in the CPIPG companies.

1.3 Lawful Bases and Personal Data Processing Purposes

The personal data processing is always based on the lawful bases, which include the consent to the personal data processing, compliance with a legal obligation, the performance of a contract, the legitimate interest, the public interest or the protection of the interests of the data subject.

1.4 Processing of Special Categories of Personal Data and Personal Data Relating to Criminal Issues

Special categories of personal data and personal data relating to criminal issues are especially sensitive and therefore a high degree of protection is applied. Any processing of special categories of personal data is consulted with the DPO.

1.5 Personal Data Transfer

The CPIPG companies may only make personal data available to third parties (including a personal data transfer within the group) under certain conditions. Personal data may only be available to a third party acting as a processor based on a personal data processing agreement. Personal data may also be available to another third-party acting as a controller or a joint-controller based on relevant contractual agreements.

In case there are requirements for rectification or erasure of the personal data or for processing restrictions, under certain circumstances, the CPIPG companies notify the relevant third parties to which the personal data were made available, unless this is not feasible or requires an inadequate effort. The CPIPG companies inform a data subject on the third parties to which the concerned personal data were disclosed, only if required to do so by the data subject.

Under certain conditions, the CPIPG companies can also transfer personal data to third countries outside the EEA or the European Union or to the international organisations. To assess legal

conditions under which personal data may be transferred to third countries or to international organisations, the CPIPG companies address the DPO for consultations.

1.6 Rights of Data Subjects

The CPIPG companies take all necessary steps to execute the rights of the data subjects stipulated by the GDPR. In respect of the personal data processing, data subjects have the rights comprising the right of access to personal data, the right to rectification, processing restriction, portability or erasure of personal data, the right to object to the personal data processing and the right not to be a subject to a decision based exclusively on the automated personal data processing.

The data subjects can request the exercise of their rights via a written or oral request. In order to provide the sufficient protection of the personal data processed by the CPIPG companies and to prevent personal data misuse from taking place, the CPIPG companies have introduced rules for the verification of the identity of the data subjects stated below.

Written request

To request the exercise of the particular right in writing, the data subjects shall fill in the request form attached to this Data Protection Policy or available from the DPO. The data subjects' signatures on the requests forms need to be officially certified. Depending on local law, data subjects may be able to have their signature certified e.g. at a notary office, post office, attorney-at-law, consulate or municipal/regional authority. The signature has to be officially certified in a country where the request is submitted to the given CPIPG company in person at the particular CPIPG company's registered seat, sent via mail using a postal services provider or verified electronic means (e.g. data boxes in Czechia). Particularly when sending the request via mail using a postal service provider in the countries outside of the EEA or the European Union, data subjects may be contacted by the given CPIPG company in order to further verify the identity.

Oral request

Data subjects may also request the exercise of their particular right in person at the given CPIPG company's registered seat. Their identity will be verified by the particular CPIPG company's designated employee (e.g. at a front desk), based on the submission of one of the following documents: personal ID card, passport or other official document with a photo sufficiently eligible to enable your clear identification.

The exercise of data subjects' rights shall not affect the rights of the third parties. Should the requests submitted by data subjects be manifestly unfounded or excessive, in particular because of the repetitive character, the CPIPG companies may require a reasonable fee, not exceeding the necessary costs of the provision of the above stated information or arranging the exercising of the data subjects' rights, for the purposes of responding to their request.

The CPIPG companies ensure sufficient communication and cooperation in order to process all received requests in adequate time. The CPIPG companies closely cooperate to provide the concerned data subject with a response within the statutory periods.

1.7 Roles and Responsibilities

The CPIPG companies and their statutory bodies are responsible for ensuring compliance with the GDPR and the relevant Member States' national data privacy legislation.

1.8 DPO

The CPIPG companies listed in the appendix have appointed a DPO with the functional and organisational responsibility for compliance with the legal regulations and internal regulations of the CPIPG companies concerning the personal data protection

The DPO can be contacted via e-mail dpo@cpipg.com or via post at the address Vladislavova 1390/17, 110 00 Praha 1, Czechia.

1.9 Responsibilities of Data Owners and of All Employees

All data owners within the CPIPG companies and all employees are obliged to process the personal data in compliance with the CPIPG companies' internal policies, the GDPR and other Member States' national data privacy legislation.

1.10 Notification of a Personal Data Breach

The CPIPG companies report any alleged breach of the personal data security to the relevant DPO immediately, in any case no later than within 24 hours. If the breach of personal data meets the requirements for reporting to the respective supervisory authority and/or data subjects, the DPO fulfils this obligation within 72 hours from the personal data breach.

1.11 Personal Data Erasure

The CPIPG companies process personal data only for a necessary time. Personal data are erased or anonymised under the following circumstances:

- Expiration of the purpose of the personal data processing without any other legitimate purpose for replacement;
- Personal data are not further needed for the purpose for which they were processed;
- Withdrawal of the data subject's consent without any other lawful basis for processing;
- Objection of the data subject against the processing without any other prevailing justified reasons; and
- Unlawful processing of the personal data.

The CPIPG companies put an emphasis on observing the necessary security measures during erasure or anonymization.

1.12 File Management

CPIPG handles documents in accordance with GDPR. The rules for receiving, registering, circulating, storing and disposing of documents in CPIPG are set out in the current CPIPG retention guidelines.

At the end of the archiving period, the documents are discarded in accordance with the established shredding procedure, with a proof of record (approval of the document owner, approval of the relevant state regional archive, certificate of shredding).

1.13 Personal Data Publishing in Public Media and the Intranet

The CPIPG companies may publish personal data in the Intranet, the Internet or any other media only with a consent of the concerned data subject, unless there is another legal basis in specific cases.

1.14 Information on Personal Data Processing

In case that CPIPG companies obtain personal data relating to data subjects directly from these data subjects, these data subjects are provided with information on the processing of their personal data at the time of obtaining such personal data. If personal data are not obtained directly from the data subjects, processing information is provided to them subsequently, mostly in the first communication with the subject.

Information on the selected processing of personal data , in cases where processing information is not available to data subjects when the personal data are obtained, it is **available here**: [Information on Personal Data Processing](#).

2. Basic Terms/Abbreviations

Data subject

An identified or identifiable individual whose personal data are processed; an identifiable individual is an individual who can be identified either directly or indirectly, predominantly with reference to a certain identifier, such as a name, identification number, location data, online identifier or one or more special elements of the physical, physiological, genetic, psychical, economic, cultural or social identity of the individual.

Data controller

A natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of personal data processing.

Processor

A natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.

Personal data

Any information on the identified or identifiable individual.

Special category

Personal data providing information on racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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 (General Data Protection Regulation).

Personal data 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.

DPO

Data Protection Officer.

Anonymised information

Information not relating to an identified or identifiable individual, including personal data anonymised so that the data subject is not or ceased to be identifiable.

Third party

Any legal entity or individual who is not the Company's employee, except for data subjects.

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.

Appendix no. 1 – List of the CPIPG companies with appointed DPO

- CPI Jihlava Shopping, a.s.
- CPI Shopping Teplice, a.s.
- CPI Shopping MB, a.s.
- CPI Národní, s.r.o.
- CB Property Development, a.s.
- CPI BYTY, a.s.
- CPI Property a Facility, s.r.o.
- CPI Services, a.s.
- Hraničář, a.s.
- Olomouc City Center, a.s.
- Best Properties South, a.s.
- OC Spektrum, s.r.o.
- CPI East,s.r.o.
- CPI Office Prague, s.r.o.
- IGY2 CB, a.s.
- Marissa Tau, a.s.
- Marissa Yellow, a.s.
- Marissa Ypsilon, a.s.
- Projekt Zlatý Anděl, s.r.o.
- Projekt Nisa, s.r.o.
- KOENIG, s.r.o.
- MB Futurum HK s.r.o.
- Buy-Way Dunakeszi Kft.
- Europeum Kft.
- Buy-Way Soroksár Kft.
- Pólus Társasház Üzemeltető Kft.
- Polus Shopping Centre
- Campona Shopping Center Kft.
- Gadwall Sp. z o.o. (Gadwall)

- Central Tower 81 Sp. z o.o. (CT81)
- CPI Poland Sp. z o. o. (CPI Poland)
- Atrium Complex
- City Gardens Sp. z o.o. (CG)
- Felicia Shopping Center SRL
- CPI Facility Slovakia, a.s.

Appendix no. 2 – Request Form

GDPR Data Subject Request Form

Notes

- Please fill this form in a readable manner.
- Incorrect, non-readable or incomplete data could cause incorrect processing or dismissal of this request.
- In order to process this request a data subject shall be clearly identified by one of the following means:
 - Verification of signature in case of written request submitted by post,
 - Identification by data subjects identification document in case of physically submitted request,
- verified electronical means (e.g. data boxes in Czechia) being sent by data subject.
- Request can be sent by postal service to the registered office of the entity being addressed by the request or physically submitted to at the registered offices within standard business hours.
- The request shall be always marked „**GDPR Request**“ (for example on an envelope), otherwise processing can be prolonged.
- In case of representation of a data subject, please provide a document based on which you represent data subject (proxy, power of attorney).
- Email is not mandatory and eases the processing of this request.

In case of any questions in relation to the GDPR requests kindly contact us by email address dpo@cpipg.com. Please be reminded that email communication is not 100% safe mean of communication and its safety, source or delivery is not guaranteed.

CPI PROPERTY GROUP

Polityka Ochrony Danych Grupy

Streszczenie

Niniejsza Polityka Ochrony Danych Grupy („**Polityka Ochrony Danych**”) wyznacza zasady ochrony danych osobowych w CPI PROPERTY GROUP („**CPIPG**”) i jej spółkach powiązanych („**Spółki CPIPG**”). Polityka Ochrony Danych ustanawia zasady ochrony danych osobowych, w tym związane z nimi obowiązki Spółek CPIPG. Polityka Ochrony Danych odzwierciedla przepisy w zakresie prywatności danych zgodnie z wymogami zawartymi w RODO, a także w ustawodawstwie pozostałych państw członkowskich dotyczących prywatności danych.

Spółki CPIPG, w swojej działalności, traktują ochronę danych osobowych poważnie i obchodzą się z nimi z odpowiednią ostrożnością i odpowiedzialnością. Naruszenie ochrony danych osobowych może nieść za sobą poważne konsekwencje prawne i ekonomiczne, zarówno dla Spółek CPIPG i ich pracowników jak i osób, których dane dotyczą. Ponadto może to zaszkodzić renomie Spółek CPIPG. Dzięki wdrożeniu Polityki Ochrony danych w Spółkach CPIPG, ryzyko wynikające z naruszenia ochrony danych osobowych zostanie zminimalizowane.

Zastosowanie

Niniejsza Polityka Ochrony Danych jest wiążąca dla Spółek CPIPG i ich pracowników. Odnosi się do wszelkiego rodzaju przetwarzania danych osobowych, do których zastosowanie mają przepisy RODO oraz ustawodawstwo państw członkowskich.

1. Procedura i Kompetencje

Poniższe postanowienia opisują procedury, których Spółki CPIPG przestrzegają w odniesieniu do przetwarzania danych osobowych. Ponadto opisują w sposób zwięzły podział kompetencji i kluczowe role w Spółkach CPIPG w obszarze przetwarzania danych osobowych.

1.1 Zobowiązanie ogólne

Spółki CPIPG podjęły i będą stale podejmować odpowiednie kroki techniczne i organizacyjne w celu zapewnienia ochrony danych osobowych przed ich niewłaściwym użyciem, utratą oraz uszkodzeniem, a także traktować je zgodnie z RODO i ustawodawstwem państw członkowskich w obszarze ochrony danych. Ochrona danych osobowych ma zastosowanie do przetwarzania danych osobowych kontrahentów Spółek CPIPG, pracowników, członków ich rodzin, kandydatów do pracy, klientów i innych osób fizycznych, których dane osobowe są przetwarzane przez Spółki CPIPG.

1.2 Podstawowe Zasady Ochrony Danych Osobowych

Spółki CPIPG przestrzegają podstawowych zasad wskazanych w RODO w odniesieniu do przetwarzania danych osobowych. Takimi zasadami ochrony danych są:

- Zasada legalności – przetwarzanie danych osobowych zawsze musi być dokonywane w oparciu o co najmniej jedną podstawę prawną;

- Zasada ograniczenia celem – dane osobowe mogą być jedynie przetwarzane dla zdefiniowanych wcześniej celów;
- Zasada minimalizacji danych – w jakimkolwiek uzasadnionym celu mogą być przetwarzane jedynie niezbędne, właściwe oraz odpowiednie dane;
- Zasada poprawności oraz transparentności – przetwarzanie musi być otwarte i transparentne dla osób, których dane dotyczą;
- Zasada integralności oraz poufności, zastosowanie zasady ścisłej potrzeby – wdrożenie niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ograniczenia dostępu do danych osobowych aby zapobiec nieuprawnionemu albo nielegalnemu przetwarzaniu;
- Zasada dokładności – przetwarzanie dokładnych i aktualnych danych osobowych;
- Reżim zarządzania kontrolowaną zmianą – zmiana istniejącego systemu przetwarzania na nowy analizowana jest przez IOD albo administratora danych i w dalszej kolejności podlega ewentualnemu sporządzeniu Oceny Skutków dla Ochrony Danych;
- Definiowanie ról uczestniczących w ochronie danych osobowych w Spółkach CPIPG.

1.3 Podstawy Prawne oraz Cele Przetwarzania Danych Osobowych

Przetwarzanie danych osobowych ma zawsze prawne podstawy, które to podstawy obejmują wymóg zgody na przetwarzanie danych osobowych, zgodność z obowiązkami prawnymi, wykonaniem umowy, uzasadnionym interesem, interesem publicznym lub ochroną interesów osób, których dane dotyczą.

1.4 Przetwarzanie Szczególnych Kategorii Danych Osobowych oraz Danych Osobowych odnoszących się do Kwestii Karnych

Szczególne kategorie danych osobowych oraz dane osobowe odnoszące się do kwestii karnych są szczególnie wrażliwe, a zatem stosuje się do nich wyższy stopień ochrony. Wszelkie przetwarzanie ww. szczególnych kategorii danych osobowych konsultowane jest z IOD.

1.5 Przekazywanie Danych Osobowych

Spółki CPIPG mogą udostępnić dane osobowe osobom trzecim (włączając w to przekazanie danych osobowych w ramach grupy) jedynie pod oznaczonymi warunkami. Dane osobowe mogą zostać udostępnione osobie trzeciej działającej jako podmiot przetwarzający jedynie w oparciu o umowę o powierzeniu przetwarzania danych osobowych. Dane osobowe mogą zostać udostępnione osobie trzeciej działającej jako administrator lub współadministrator w oparciu o właściwe porozumienia umowne.

W przypadku wymogu skorygowania albo usunięcia danych osobowych albo ograniczenia przetwarzania, w pewnych okolicznościach, Spółki CPIPG poinformują o tym właściwe osoby trzecie, którym udostępniono dane osobowe, chyba że nie jest to wykonalne albo wiąże się z nieadekwatnym wysiłkiem. Spółki CPIPG poinformują osobę, której dane dotyczą o osobach trzecich, którym takie dane osobowe zostały ujawnione, jedynie jeżeli zażąda tego osoba, której dane dotyczą.

Spółki CPIPG mogą również, pod pewnymi warunkami, przekazywać dane osobowe krajom spoza EOG albo Unii Europejskiej lub organizacjom międzynarodowym. Aby ocenić prawne warunki, w oparciu o które dane osobowe

mogą być przekazywane do krajów trzecich albo do organizacji międzynarodowych, Spółki CPIPG kontaktują się z IOD w celu przeprowadzenia konsultacji.

1.6 Prawa Osób, których Dane Dotyczą

Spółki CPIPG podejmują wszelkie niezbędne kroki w celu wykonania praw osób, których dane dotyczą wskazanych w RODO. W odniesieniu do przetwarzania danych osobowych, osoby, których dane dotyczą posiadają prawo dostępu do danych osobowych, prawo sprostowania, ograniczenia przetwarzania, przenoszenia albo usuwania danych osobowych, prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych oraz prawo do niepodlegania wyłącznie zautomatyzowanemu podejmowaniu decyzji w zakresie przetwarzania danych osobowych.

Osoby, których dane dotyczą mogą żądać wykonania ich praw w drodze wniosku ustnego lub pisemnego. W celu zapewnienia właściwej ochrony danych osobowych przetwarzanych przez Spółki CPIPG oraz aby zapobiec nieprawidłowemu wykorzystaniu, Spółki CPIPG wprowadziły zasady weryfikacji tożsamości osób, których dane dotyczą, o których mowa poniżej.

Wniosek pisemny

Osoba, której dane dotyczą żądająca wykonania danego prawa na piśmie, wypełnia wniosek którego wzór został dołączony do niniejszej Polityki Ochrony Danych lub który może pobrać u IOD. Podpis osoby, której dane dotyczą na wniosku musi zostać poświadczony urzędowo. Zależnie od lokalnego prawa, osoba, której dane dotyczą może uzyskać poświadczenie podpisu na przykład u notariusza, na poczcie, przez adwokata, w konsulacie lub w urzędzie władz miejskich/samorządowych. Podpis musi zostać urzędowo potwierdzony w kraju, w którym: wniosek jest składany Spółce CPIPG osobiście w siedzibie danej Spółki CPIPG, nadany pocztą za pośrednictwem dostawcy usług pocztowych lub za pomocą uwierzytelnionych środków elektronicznych (na przykład data boxes w Czechach). W szczególności w przypadku nadania wniosku drogą pocztową za pośrednictwem dostawcy usług pocztowych w kraju spoza EOG albo spoza Unii Europejskiej, Spółka CPIPG może skontaktować się z osobami, których dane dotyczą w celu dodatkowego zweryfikowania tożsamości.

Wniosek ustny

Osoby, których dane dotyczą mogą ponadto żądać wykonania swoich danych praw osobiście we właściwej siedzibie Spółki CPIPG. Tożsamość takich osób zostanie zweryfikowana przez wyznaczonego pracownika Spółki CPIPG (np. w recepcji), na podstawie okazania jednego z następujących dokumentów tożsamości: dowód osobisty, paszport albo inny dokument urzędowy ze zdjęciem wystarczająco czytelnym aby umożliwić wyraźną identyfikację.

Wykonanie praw osób, których dane dotyczą nie wpływa na prawa osób trzecich. Jeżeli wniosek osoby, której dane dotyczą będzie wyraźnie bezzasadny albo nadmierny, w szczególności ze względu na jego powtarzający się charakter, Spółki CPIPG mogą pobierać zasadną opłatę, nie przekraczającą niezbędnych kosztów udzielenia powyższych informacji lub zorganizowania wykonania praw osób, których dane dotyczą, w celu udzielenia odpowiedzi na ich wniosek.

Spółki CPIPG zapewniają wystarczający stopień komunikacji i współpracy w celu przetworzenia wszystkich otrzymanych wniosków w odpowiednim czasie. Spółki CPIPG ściśle współpracują ze sobą aby dana osoba, której dane dotyczą uzyskała odpowiedź w okresie ustalonym przepisami prawa.

1.7 Role i Obowiązki

Za zapewnienie zgodności z RODO oraz właściwym ustawodawstwem państw członkowskich w zakresie ochrony danych odpowiedzialne są Spółki CPIPG oraz ich organy statutowe.

1.8 IOD

Spółki CPIPG wymienione w załączniku powołały IOD, który ponosi funkcjonalną i organizacyjną odpowiedzialność za zgodność z regulacjami prawnymi i wewnętrznymi spółek CPIPG w zakresie ochrony danych osobowych.

Kontakt z IOD jest możliwy za pośrednictwem poczty elektronicznej pod adresem dpo@cpipg.com albo poczty na adres Vladislavova 1390/17, 110 00 Praha 1, Czechy.

1.9 Obowiązki Właścicieli Danych i Wszystkich Pracowników

Wszyscy właściciele danych w Spółkach CPIPG oraz wszyscy pracownicy są zobowiązani do przetwarzania danych osobowych zgodnie z wewnętrznymi politykami Spółek CPIPG, RODO oraz odpowiednim ustawodawstwem państw członkowskich w zakresie ochrony danych osobowych.

1.10 Powiadomianie o Naruszeniu Ochrony Danych Osobowych

Spółki CPIPG niezwłocznie informują właściwego IOD o jakimkolwiek domniemanym naruszeniu ochrony danych osobowych, w każdym przypadku nie później niż w ciągu 24 godzin. Jeżeli naruszenie ochrony danych osobowych spełnia wymogi raportowania właściwym władzom nadzorczym lub osobie, której dane dotyczą, IOD wypełnia obowiązek takiego raportowania w ciągu 72 godzin od naruszenia ochrony danych osobowych.

1.11 Usuwanie Danych Osobowych

Spółki CPIPG przetwarzają dane osobowe wyłącznie w niezbędnym okresie. Dane osobowe zostają usunięte albo zanonimizowane w następujących okolicznościach:

- Cel, na jaki dane osobowe były przetwarzane wygaśnie oraz nie istnieje już żaden inny uzasadniony cel;
- Dane osobowe nie są już potrzebne na cele, na jakie były przetwarzane;
- Osoba, której dane dotyczą wycofa swoją zgodę i nie istnieje już inna prawna podstawa przetwarzania;
- Osoba, której dane dotyczą sprzeciwia się przetwarzaniu, a nie istnieją przeważające uzasadnione przyczyny przetwarzania; albo
- Dane osobowe są przetwarzane bezprawnie.

W trakcie usuwania albo zanonimizowania Spółki CPIPG kładą szczególny nacisk na przestrzeganie koniecznych środków ostrożności.

1.12 Publikowanie Danych Osobowych w Mediach Publicznych oraz Intranecie

Publikowanie danych osobowych przez Spółki CPIPG w Intranecie, Internecie albo innych mediach jest dozwolone jedynie za zgodą odpowiedniej osoby, której dane dotyczą, chyba że istnieje inna podstawa prawna w szczególnych sytuacjach.

2. Podstawowe terminy/ skróty

Osoba, której dane dotyczą	Osoba fizyczna zidentyfikowana lub możliwa do zidentyfikowania, której dane osobowe są przetwarzane; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio 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 danej osoby.
Administrator danych	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
Podmiot Przetwarzający	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot przetwarzający dane osobowe w imieniu administratora danych.
Dane osobowe	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
Szczególna kategoria	Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
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 (Ogólne Rozporządzenie o Ochronie Danych).
Przetwarzanie danych osobowych	Każda operacja lub zestaw operacji wykonywanych na danych osobowych albo na zestawach danych osobowych w sposób zautomatyzowany lub inny, jak np. zbieranie, utrwalanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
IOD	Inspektor Ochrony Danych.

25 maja 2018 roku

Informacje zanonimizowane Informacje nie odnoszące się do zidentyfikowanej lub dającej się zidentyfikować osoby fizycznej, w tym dane osobowe zanonimizowane w taki sposób, że osoba, której dane dotyczą nie jest albo przestała być możliwa do zidentyfikowania..

Osoba trzecia Jakikolwiek podmiot prawny albo osoba fizyczna, która nie jest pracownikiem Spółki, z wyjątkiem osób, których dane dotyczą.

Zgoda Każde dobrowolnie udzielone, konkretne i świadome wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych, w formie oświadczenia albo przez jasne twierdzące wskazanie.

Załącznik nr 1 – Lista Spółek CPIPG, w których powołano Inspektora Ochrony Danych

- CPI Jihlava Shopping, a.s.
- CPI Shopping Teplice, a.s.
- CPI Shopping MB, a.s.
- CPI Národní, s.r.o.
- CB Property Development, a.s.
- CPI BYTY, a.s.
- CPI Property, s.r.o.
- CPI Services, a.s.
- Hraničář, a.s.
- Olomouc City Center, a.s.
- Best Properties South, a.s.
- OC Spektrum, s.r.o.
- CPI East, s.r.o.
- CPI Office Prague, s.r.o.
- IGY2 CB, a.s.
- Marissa Tau, a.s.
- Marissa Yellow, a.s.
- Marissa Ypsilon, a.s.
- CPI Hotels, a.s.
- Projekt Zlatý Anděl, s.r.o.
- Projekt Nisa, s.r.o.
- KOENIG, s.r.o.
- MB Futurum HK s.r.o.
- Gewerbesiedlungs-Gesellschaft mbH
- Buy-Way Dunakeszi Kft.
- Europeum Kft.
- Buy-Way Soroksár Kft.
- CPI Hotels Hungary Kft.
- Pólus Társasház Üzemeltető Kft.
- Campona Shopping Center Kft.
- Suncani Hvar d.d.
- Gadwall Sp. z o.o. (Gadwall)
- Central Tower 81 Sp. z o.o. (CT81)
- CPI Poland Sp. z o. o. (CPI Poland)
- CPI Hotels Poland sp. z o.o.
- City Gardens Sp. z o.o. (CG)
- Felicia Shopping Center SRL
- CPI Facility Slovakia, a.s.
- CPI Hotels Slovakia, s. r. o.

Załącznik nr 2 – Wzór wniosku

RODO - Wzór wniosku osoby, której dane dotyczą

Identyfikacja podmiotu, który jest adresatem niniejszego wniosku

Numer identyfikacyjny:	Nazwa Spółki:
------------------------	---------------

Identyfikacja osoby, której dane dotyczą / przedstawiciela

Imię:	Nazwisko:	Tytuł:
Data urodzenia:	Imię i nazwisko nadane w chwili urodzenia:	
Miasto	Kraj:	Kod:
Ulica:	Numer domu:	
Rodzaj dokumentu tożsamości:		
Numer identyfikacyjny dokumentu tożsamości:		

Identyfikacja przedstawiciela osoby, której dane dotyczą (wypełnić wyłącznie w przypadku przedstawiciela)

Imię:	Nazwisko:	
Nazwa Spółki:		
Data urodzenia:	PESEL:	Kraj:
Miasto	Kod:	
Ulica	Numer:	
Reprezentowany/a przez <input type="checkbox"/> Dokument <input type="checkbox"/> Określić: pełnomocnika		

Dodatkowa identyfikacja (nie jest wymagana)

Email:

Opis wniosku osoby, której dane dotyczą (o co wnosi osoba, której dane dotyczą)

Data:

Potwierdzony podpis:

Uwagi

- Prosimy o czytelne wypełnienie wniosku.
- Dane nieprawidłowe, nieczytelne albo niekompletne mogą spowodować nieprawidłowe przetworzenie lub odrzucenie niniejszego wniosku.
- W celu przyjęcia do rozpatrzenia niniejszego wniosku osoba, której dane dotyczą zostanie wyraźnie zidentyfikowana za pomocą:
 - Weryfikacji podpisu w przypadku pisemnego wniosku przesłanego pocztą,
 - Identyfikacji na podstawie dokumentu tożsamości osoby, której dane dotyczą w przypadku fizycznego doręczenia wniosku,
 - Sprawdzonej środków komunikacji elektronicznej (np. za pomocą data boxes w Czechach) przesyłanych przez osobę, której dane dotyczą.
- Wniosek można przesłać za pośrednictwem poczty na adres siedziby podmiotu, który jest adresatem wniosku lub doręczyć osobiście w jego siedzibie w godzinach pracy biura.
- Wniosek należy zawsze oznaczyć „**Wniosek RODO**” (przykładowo na kopercie), w przeciwnym razie rozpatrywanie wniosku może trwać dłużej.
- Jeżeli osoba, której dane dotyczą korzysta z pełnomocnika, prosimy o okazanie dokumentu na podstawie którego osoba, której dane dotyczą jest reprezentowana (upoważnienie, pełnomocnictwo).
- Mail nie jest obowiązkowy ale ułatwia rozpatrywanie wniosku.

W razie jakichkolwiek pytań dotyczących wniosków RODO uprzejmie prosimy o kontakt pod adresem mailowym dpo@cpipg.com. Jednocześnie przypominamy, że komunikacja mailowa nie jest bezpieczna w 100% i nie gwarantuje się jej bezpieczeństwa, źródła ani doręczenia.