Umowa o zachowaniu poufności zawarta w Gdańsku, między:	**Non-disclosure Agreement** concluded in Gdańsk, between:
ERGO Technology & Services S.A., z siedzibą w Gdańsku, ul. Droszyńskiego 24, 80-381 Gdańsk, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000438903 przez Sąd Rejonowy Gdańsk-Północ w Gdańsku, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, NIP585-10-07-625, o kapitale zakładowym w wysokości 1.303.000 zł opłaconym w całości, posiadająca status dużego przedsiębiorcy w rozumieniu ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych, reprezentowana przez: 1. _____, 2. _____, - zwaną dalej "**ET&S**" -.	**ERGO Technology & Services S.A.,** with its registered office in Gdańsk, Poland, ul. Droszyńskiego 24, 80-381 Gdańsk, entered into the register of entrepreneurs of the National Court Register under KRS no. 0000438903 by the District Court Gdańsk-Północ in Gdańsk, VIII Commercial Division of the National Court Register, Tax identification No. (NIP) 585-10-07-625, with the share capital of PLN 1,303,000 paid up in full, a large enterprise within the meaning of Act of March 8th, 2013 on countering excessive payment delays in commercial transactions, represented by: 1. _____, 2. _____, - hereinafter referred to as „**ET&S**“ -
oraz …….. z siedzibą w …….. wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: …….. przez Sąd Rejonowy …….. Wydział Gospodarczy Krajowego Rejestru Sądowego, NIP …….. o kapitale zakładowym …….. złotych wpłaconym w całości, reprezentowaną przez: 1. _____, 2. _____, - zwanym dalej "**Odbiorcą informacji**" -	and …….. with its registered office in …….. entered into the register of entrepreneurs of the National Court Register under KRS no. …….. by the District Court …….. Commercial Division of the National Court Register, Tax identification No. (NIP) …….. with the share capital of PLN …….. paid up in full, represented by: 1. _____, 2. _____, - hereinafter referred to as „**Information receiver**” -

- oba podmioty łącznie zwane dalej "**Stronami** " a osobno „**Stroną**"-	- both collectively hereinafter referred to as "**the Parties**" and individually as "**the Party**" -
1. Zakres, przedmiot W związku z badaniem możliwości współpracy lub negocjowaniem umów lub zaproszeniem do składania ofert lub dostarczaniem przez Odbiorcę informacji towarów lub wykonywaniem prac lub usług na rzecz ET&S, ET&S może udostępnić Odbiorcy informacji informacje poufne. Celem niniejszej umowy o zachowaniu poufności (zwanej dalej "Umową") jest ochrona informacji poufnych. ET&S nie jest jednak zobowiązane do udzielania informacji poufnych. Poniższe postanowienia mają zastosowanie w przypadku przekazania Odbiorcy informacji, informacji poufnych przez ET&S, podmiot powiązany z ET&S tj. każdy inny podmiot bezpośrednio lub pośrednio kontrolujący, kontrolowany przez lub znajdujący się pod wspólną kontrolą z ET&S, gdzie dla celów niniejszego dokumentu "kontrola" oznacza posiadanie, bezpośrednio lub pośrednio, większości udziałów lub praw do głosowania w danym podmiocie lub uprawnień do kierowania lub kontroli nad zarządzaniem lub polityką danego podmiotu, w każdym przypadku bezpośrednio lub pośrednio poprzez posiadanie papierów wartościowych lub udziałów lub innych praw własności, na podstawie stosownej umowy lub w inny sposób (dalej zwane "Podmiotami powiązanymi[1]") lub przez osoby trzecie (np. konsultantów) w imieniu ET&S lub jego Podmiotów powiązanych. Umowa dotyczy wszystkich obecnych i przyszłych przetargów, umów i zamówień składanych przez ET&S lub jego Podmioty powiązane, w których uczestniczy	**1. Scope, subject matter** In connection with the examination of a cooperation and/or contract negotiations and/or an invitation to tender and/or deliveries of goods and/or works or services, ET&S may make confidential information available to the Information receiver. The purpose of this non-disclosure agreement (hereinafter referred to as "this Agreement") is to protect confidential information. However, ET&S is not obliged to provide confidential information. The following provisions apply if confidential information is provided to the Information receiver by ET&S, a company affiliated with ET&S i.e. any other entity directly or indirectly controlling, controlled by, or under common control with ET&S, where for the purposes hereof, "control" means the possession, whether directly or indirectly, of the majority of shares or voting rights in or of the power to direct or cause the direction of management or policies of given entity, in each case whether directly or indirectly and whether through the ownership of securities or partnership or other ownership interests, by appropriate contract or otherwise (hereinafter referred to as "Affiliates[1]") or by third parties (e.g. consultants) on behalf of ET&S or its Affiliates. This Agreement applies to all current and future calls for tender, contracts and mandates by ET&S or its Affiliates

[1] *W odniesieniu do ET&S będzie to każdy podmiot należący do grupy kapitałowej MunichRe, w szczególności, ale nie wyłącznie/In relation to ET&S, this will be any entity belonging to the MunichRe capital group, in particular, but not exclusively: ERGO Group AG, ERGO Technology & Services Management AG, ITERGO Informationstechnologie GmbH, ERGO Technology & Services Private Limited, ERGO Direkt AG, Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A., Sopockie Towarzystwo Ubezpieczeń na Życie ERGO Hestia S.A.*

Odbiorca informacji lub zawartych z Odbiorcą informacji umów na usługi. Umowa nie uprawnia Odbiorcy informacji do uwzględnienia go w zaproszeniach do składania ofert lub przy udzielaniu zamówień na usługi.	in which the Information receiver participates. It does not entitle the Information receiver to be taken into account in invitations to tender or in the award of services.
2. Informacje poufne Informacjami poufnymi w rozumieniu Umowy (zwanymi dalej "informacjami poufnymi ") są: a) Wszelkie informacje technologiczne, biznesowe, finansowe, operacyjne, strategiczne lub inne dotyczące ET&S i jego Podmiotów powiązanych lub ich klientów, kontrahentów, partnerów biznesowych, konsultantów, członków organów lub pracowników, w szczególności dotyczące organizacji, procesów technologicznych i danych, systemu, oprogramowania, dokumentacji, praw własności intelektualnej, produktów, wynalazków, działania, metodologii, procesów, know-how, licencje, plany, ceny, tajemnice handlowe i strategie handlowe, treść rozmów handlowych i konsultacji technologicznych, a także treść zawartych umów oraz dane osobowe, uzyskane przez Odbiorcę informacji (niezależnie od formy przekazania tych informacji i ich źródła), jak i inne, ujawnione Odbiorcy informacji w związku z realizowaną współpracą, uzyskane w formie ustnej, pisemnej, elektronicznej lub w jakikolwiek inny sposób i w jakiejkolwiek formie w ramach zaproszeń do składania ofert, realizacji zamówień, w ramach prowadzonych rozmów lub w związku z realizacją umów o współpracy, niezależnie od tego, czy informacje są oznaczone jako poufne czy nie. Przekazywanie informacji poufnych może odbywać się w formie pisemnego powiadomienia, przekazania nośników informacji, upoważnienia do dostępu do informacji (np. do banku danych), ustnie, poprzez przekazanie próbek/materiałów	**2. Confidential Information** Confidential information within the meaning of this Agreement (herein after referred to as “confidential information”) are: a) Any technological, business, financial, operational, strategic or other information about ET&S and its Affiliates or about its customers, contractors, business partners, consultants, directors or employees, particularly regarding organization, technological processes and data, system, software, documentation, intellectual property rights, products, inventions, operation, methodology, processes, know-how, licences, plans, prices, trade secret and commercial strategies, content of business conversations and technological consultations, as well as content of concluded agreements and personal data obtained by the Information receiver (regardless of the form of providing this information and its source), as well as other information disclosed to the Information receiver in connection with the cooperation, obtained orally, in writing, electronically or in any other way and in any form within the framework of invitations to tender, mandates or in a joint dialogue or in connection with implementation of cooperation agreements, regardless of whether the information is marked as confidential or not. The transmission of confidential information may take place by written notification, handover of information carriers, authorization to access information (e.g. to a data bank), orally, by handover of samples/test material/products or by visual/electronic transmission.

testowych/produktów lub poprzez przekaz wizualny/elektroniczny. b) Okoliczność, że Strony badają możliwość współpracy, prowadzą negocjacje kontraktowe, biorą udział w przetargu lub wymieniają się dostawami towarów lub wykonywaniem prac lub usług.	b) The circumstance that the Parties examine a cooperation, conduct contract negotiations, are involved in an invitation to tender and/or exchange deliveries of goods and/or works or services.
3. Obowiązek zachowania poufności Jeżeli ust. 4 nie stanowi inaczej, Odbiorca informacji jest obowiązany do: a) zachowania w tajemnicy informacji poufnych i nieujawniania ich osobom trzecim bez uprzedniej pisemnej zgody ET&S; b) ochrony informacji poufnych przed publikacją i ujawnieniem; c) wykorzystywania informacji poufnych tylko do wewnętrznych celów badania możliwości współpracy lub w kontekście odpowiedniego zaproszenia do składania ofert lub realizacji odpowiedniego stosunku umownego i tylko w niezbędnym zakresie; d) udostępnienia informacji poufnych tylko tym pracownikom, organom, przedstawicielom, konsultantom lub innym osobom działającym na jego zlecenie, które bezwzględnie potrzebują dostępu do informacji poufnych i ich oceny w ramach przetargu lub umowy ("zasada need-to-know"); e) ujawniania informacji poufnych osobom uprawnionym na podstawie pkt 3 lit. d) tylko w zakresie niezbędnym z uwagi na toczące się rozmowy i/lub zaproszenia do składania ofert i/lub w ramach odpowiedniego wykonania umowy; f) nie kopiować, nie powielać ani w żaden inny sposób nie utrwalać i nie rozpowszechniać informacji poufnych lub ich części, z wyjątkiem	**3. Confidentiality obligation** Unless otherwise provided for in paragraph 4, the Information receiver is obliged: a) to keep confidential information secret and not to disclose it to third parties without ET&S's prior written consent; b) to protect confidential information against publication and disclosure; c) to use confidential information only for internal purposes of the examination of a cooperation and/or in the context of the respective invitation to tender and/or implementation of the respective contractual relationship and only to the necessary extent; d) to make the confidential information available only to those employees, bodies, representatives, consultants or other vicarious agents who absolutely need access to the confidential information and its evaluation within the scope of the tender or contract ("need-to-know principle"); e) to disclose confidential information to the persons entitled under paragraph 3. lit. d) only to the extent necessary in view of the discussions and/or invitations to tender that are taking place and/or within the framework of the respective execution of the contract. f) not to copy, reproduce or in any other way record or disseminate confidential information or parts thereof, except for cases when it is necessary to

przypadków, gdy jest to konieczne w celu realizacji współpracy lub w innym celu ściśle związanym z przedmiotem współpracy Stron, w których to przypadkach wszelkie kopie lub reprodukcje informacji poufnych utrwalonych na jakichkolwiek nośnikach informacji, łącznie z nośnikami elektronicznymi, pozostają własnością ET&S. Powielanie lub zwielokrotnianie nośników informacji poufnych wymaga pisemnej zgody ET&S.	implement cooperation or for other purposes closely related to the subject of cooperation of the Parties, in which cases all copies or reproductions of confidential information recorded on any information carriers, including electronic carriers, remain the property of ET&S. Reproduction or multiplication of confidential information carriers requires ET&S's written consent.
g) stosować zasady klasyfikacji informacji poufnych określone w Załączniku nr 1 do Umowy.	g) apply the principles of classification of confidential information specified in Annex No. 1 to the Agreement.
Ponadto Odbiorca informacji musi zobowiązać osoby, które są uprawnione do otrzymania informacji poufnych na podstawie Umowy, do zachowania poufności w zakresie określonym powyżej i jest odpowiedzialny za przestrzeganie obowiązków wynikających z Umowy przez te osoby, tak jakby one same były zobowiązane na podstawie Umowy. Dla celów Umowy, wszelkie działania lub zaniechania osób, o których mowa w punkcie 3 lit. d), uznaje się za własne działania lub zaniechania Odbiorcy informacji.	In addition, the Information receiver must oblige persons who are entitled to receive confidential information under this Agreement, to confidentiality to the extent specified above and is responsible for compliance with the obligations arising from this Agreement by such persons as if they themselves were obligated under this non-disclosure agreement. For the purposes of this Agreement, any actions or omissions of the persons referred to in Section 3 lit. d) shall be deemed to be the Information receivers own actions or omissions.
Odbiorca informacji jest zobowiązany do niezwłocznego poinformowania ET&S na adres: security-report@ergo.com, jeżeli dowiedział się o naruszeniu poufności przez osobę fizyczną lub prawną lub jednostkę organizacyjną niebędącą osobą prawną, której przepisy szczególne przyznają zdolność prawną, której przekazał informacje poufne lub ich części lub o których dowiedziała się w sposób nieuprawniony. Odbiorca informacji zapewni ET&S wszelkie wsparcie, jakiego można racjonalnie oczekiwać w każdym działaniu, jakie ET&S lub jego Podmioty powiązane zainicjują przeciwko takiej osobie fizycznej lub prawnej lub jednostce organizacyjnej niebędącej osobą prawną, której przepisy szczególne przyznają zdolność prawną z powodu naruszenia poufności.	The Information receiver is obliged to inform ET&S immediately at: security-report@ergo.com if he learns of a breach of confidentiality by a natural or legal person or an organizational entity that is not a legal person, which is granted legal capacity by special regulations to whom it has passed on confidential information or parts thereof or which it has learned of it in an unauthorized manner. The Information receiver shall provide ET&S with all the support that can reasonably be expected in any action that ET&S or its Affiliates will initiate against such a natural or legal person, or an organizational entity that is not a legal person, which is granted legal capacity by special regulations, on account of a breach of confidentiality.
4. Wyłączenia	**4. Exceptions**

Nie ma obowiązku zachowania w tajemnicy informacji poufnych, pod warunkiem, że: a) Odbiorca informacji znał informacje poufne przed ich ujawnieniem przez ET&S lub jakąkolwiek firmę lub osobę, o której mowa w pkt 1 i jest to możliwe do wykazania, lub b) informacje poufne były znane lub publicznie dostępne przed ich ujawnieniem i jest to możliwe do wykazania; lub c) informacja poufna w sposób możliwy do zweryfikowania stała się znana lub ogólnie dostępna po przekazaniu jej Odbiorcy informacji bez udziału lub winy Odbiorcy informacji; lub d) informacje poufne zostały ujawnione lub udostępnione Odbiorcy informacji w dowolnym czasie przez osobę trzecią upoważnioną do ich przekazania i jest to możliwe do wykazania, lub e) w sposób możliwy do zweryfikowania, ET&S wyraził zgodę w formie pisemnej na ujawnienie informacji poufnych osobom trzecim zgodnie z niniejszym zobowiązaniem do zachowania poufności. Jeżeli Odbiorca informacji jest zobowiązany przepisami prawa lub nakazem sądu lub właściwego organu do ujawnienia informacji poufnych, obowiązek zachowania poufności nie ma zastosowania jedynie w zakresie, w jakim ujawnienie informacji poufnych jest absolutnie niezbędne do wykonania bezwzględnie obowiązujących przepisów prawa lub nakazu. W takim przypadku Odbiorca informacji jest zobowiązany do niezwłocznego poinformowania ET&S na piśmie i w porozumieniu z ET&S do podjęcia wszelkich uzasadnionych działań w celu odmowy ujawnienia lub zapewnienia poufności informacji przed jej ujawnieniem.	There is no obligation to keep confidential information confidential, provided that: a) the Information receiver was demonstrably aware of the confidential information prior to disclosure by ET&S or any company or person referred to in paragraph 1, or b) the confidential information were demonstrably known or publicly available to the public prior to disclosure; or c) the confidential information verifiably became known or generally accessible to the public after notification without the involvement or fault of the Information receiver; or d) the confidential information have been demonstrably disclosed or made accessible to the Information receiver at any time by a third party authorized to pass them on, or e) the confidential information have been verifiably released by ET&S in writing for disclosure to third parties in accordance with this confidential obligation. If the Information receiver is required by law or by an order of a court or competent authority to disclose confidential information, the obligation of confidentiality shall not apply only to the extent that the disclosure of confidential information is absolutely necessary to comply with the mandatory law or order. In such a case, the Information receiver is obliged to inform ET&S immediately in writing and, in agreement with ET&S, to take all reasonable measures to reject disclosure requirements and/or to ensure the confidentiality of the information prior to disclosure.
5. Ochrona danych i obowiązki wynikające z przepisów prawa Odbiorca informacji zobowiązany jest do przestrzegania przepisów Rozporządzenia Parlamentu Europejskiego i	**5. Data protection and obligation according to law** The Information receiver is obliged to comply with the provisions of the Regulation (EU) 2016/679 of the

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 (RODO) oraz innych obowiązujących przepisów dotyczących ochrony danych w zakresie swoich kompetencji.	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 (GDPR) and other applicable data protection regulations within its area of responsibility.
Jeżeli Odbiorca informacji przyjmuje również zadania dla ubezpieczycieli jako podwykonawca ET&S, Odbiorca informacji przyjmuje do wiadomości, iż informacje dotyczące umów ubezpieczenia, w posiadanie których wszedł w związku z realizacją usług zleconych przez ET&S objęte są tajemnicą ubezpieczeniową wynikającą z art. 35 ust. 1 Ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (tajemnica ubezpieczeniowa) oraz, że osoby i podmioty za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe są zobowiązane do przestrzegania tajemnicy ubezpieczeniowej z zachowaniem wszelkich konsekwencji związanych z niedopełnieniem tego obowiązku.	If the Information receiver also assumes tasks for insurers as a subcontractor of ET&S, the Information receiver acknowledges that the information regarding insurance contracts that it came into possession of in connection with the performance of services commissioned by ET&S is covered by insurance secrecy under Article 35(1) of the Insurance and reinsurance activity act of September 11, 2015 (insurance secrecy), and that, individuals and entities through which the insurance company performs insurance activities are obligated to observe insurance secrecy with all consequences associated with failure to do so.
ET&S poinformowało Odbiorcę informacji, że osoby zobowiązane do zachowania tajemnicy ubezpieczeniowej podlegają odpowiedzialności karnej zgodnie z art. 439 Ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej w przypadku ujawnienia lub wykorzystania tajemnicy ubezpieczeniowej.	ET&S has informed the Information receiver that that persons obligated to maintain insurance secrecy are subject to criminal liability under Article 439 of the Insurance and reinsurance activity act of September 11, 2015 in the event of disclosure or use of insurance secrecy.
Odbiorca informacji zobowiązuje się do przestrzegania obowiązku zachowania poufności i traktowania wszystkich informacji wymagających zachowania poufności jako ściśle tajnych. Ponadto Odbiorca informacji zobowiąże swoich pracowników do zachowania poufności i poinformuje ich o konsekwencjach karnych naruszenia.	The Information receiver undertakes to observe the duty of confidentiality and to treat all information requiring confidentiality as strictly confidential. In addition, the Information receiver will oblige his employees to maintain confidentiality and inform them of the criminal consequences of a violation.
Odbiorca informacji uzyska wiedzę o tajemnicy ubezpieczeniowej tylko w takim zakresie, w jakim jest to	

niezbędne do wypełnienia przyjętych przez niego zadań umownych. Jeżeli Odbiorca informacji korzysta z usług podwykonawców w celu realizacji zadań dla ET&S lub Podmiotów powiązanych, zobowiąże ich również do zachowania tajemnicy i wskaże na prawnokarne konsekwencje jej naruszenia. Odbiorca informacji uzgodni w umowie z podwykonawcą, że podwykonawca zobowiąże swoich pracowników do zachowania poufności i wskaże na prawnokarne konsekwencje naruszenia. Odbiorca informacji jest zobowiązany poinformować swoich pracowników, przedstawicieli, konsultantów lub inne osoby działające na jego zlecenie, których dane osobowe będą przekazywane ET&S, w sprawie przetwarzania ich danych w związku z zaproszeniem do składania ofert lub realizacją odpowiedniego stosunku umownego z ET&S. Klauzula informacyjna ET&S dotycząca przetwarzania danych osobowych dostępna jest na stronie internetowej https://www.ET&S.com/pl-PL/Microsites/ETS/Start/Privacy-statement a Odbiorca informacji potwierdza jej otrzymanie i zobowiązuje się do przekazania jej swoim pracownikom, przedstawicielom, konsultantom lub innym osobom działającym na jego zlecenie, których dane osobowe będą przekazywane ET&S.	The Information receiver will only obtain knowledge of insurance secrets to the extent that this is necessary for the fulfilment of the contractual tasks assumed by him. If the Information receiver uses other subcontractors to fulfil the tasks he has assumed in order to provide services to ET&S or its Affiliates, he will also oblige them to secrecy and point out the criminal law consequences of a violation. The Information receiver shall contractually agree with the subcontractor that he shall oblige his employees to maintain confidentiality and point out the criminal law consequences of an infringement. The Information receiver is obliged to inform its employees, representatives, consultants or other vicarious agents whose personal data will be provided to ET&S, on processing their data in relation to respective invitation to tender and/or implementation of the respective contractual relationship with ET&S. ET&S's Information clause regarding processing personal data is available on the website https://www.ET&S.com/pl-PL/Microsites/ETS/Start/Privacy-statement and the Information receiver confirms its receipt and undertakes to pass it on to employees, representatives, consultants or other vicarious agents whose personal data will be provided to ET&S.
6. Zwrot informacji poufnych W przypadku braku podjęcia współpracy po odpowiednim zaproszeniu do składania ofert lub w przypadku niepowodzenia negocjacji umownych lub rozwiązania odpowiedniego stosunku umownego lub na pisemne żądanie ET&S, Odbiorca informacji jest zobowiązany: a) zniszczyć lub zwrócić ET&S wszystkie dokumenty i wszystkie inne materiały (w tym materiały komputerowe) lub ich części, które zawierają lub odzwierciedlają informacje poufne,	**6. Return of confidential information** If there is no cooperation after the respective invitation to tender and/or in the event of failure of contractual negotiations and/or termination of the respective contractual relationship and/or at ET&S's written request, the Information receiver is obliged to: a) destroy or return to ET&S all documents and all other materials (including computer material) or parts thereof which contain or reflect confidential information, together with all copies and records

wraz ze wszystkimi kopiami i zapisami będącymi w posiadaniu lub pod kontrolą Odbiorcy informacji lub jego doradców i pracowników, a które są w formie, która może być wydana lub zniszczona; oraz b) usunąć wszystkie informacje poufne z wszystkich komputerów lub podobnych urządzeń, w których informacje poufne były przechowywane przez Odbiorcę informacji lub osoby działające na jego zlecenie. Na żądanie ET&S Odbiorca informacji jest zobowiązany niezwłocznie, nie później niż w terminie 3 dni od dnia otrzymania takiego żądania, potwierdzić na piśmie wykonanie obowiązków określonych w pkt 6 a) i b).	in the possession or under the control of the Information receiver or its advisers and employees and which are in a form which may be issued or destroyed; and b) delete all confidential information from all computers or similar devices in which confidential information was stored by the Information receiver or his vicarious agents. At ET&S's request, the Information receiver must immediately, no later than 3 days as of the day of receiving such request, confirm in writing that it has fulfilled the obligations set out in paragraph 6 a) and b).
7. Zrzeczenie się odpowiedzialności, Prawa ET&S nie ponosi odpowiedzialności za straty wynikające z wykorzystania informacji poufnych przekazanych w ramach Umowy. Ani Umowa, ani informacje poufne udostępnione w ramach Umowy nie przyznają żadnych praw własności przemysłowej (w tym patenty) ani żadnych praw do używania i wykorzystywania informacji chronionych prawem autorskim. ET&S lub jego Podmioty powiązane pozostają właścicielem praw do informacji poufnych przekazanych lub podanych do wiadomości Odbiorcy informacji.	**7. Disclaimer, Rights** ET&S is not liable for losses arising from the use of confidential information transmitted under this Agreement. No licenses for industrial property rights (including patents) and no rights of use and exploitation for information protected by copyright are neither granted by this Agreement nor by confidential information made available within the scope of this Agreement. ET&S and/or its Affiliates remains the owner of the rights to the confidential information transmitted to or brought to the knowledge of the Information receiver.
8. Podwykonawcy, osoby działające na zlecenie Jeżeli Odbiorca informacji zamierza skorzystać z usług osób działających na jego zlecenie lub podwykonawców w ramach współpracy, która ma zostać podjęta przez Strony lub w ramach realizacji stosunku umownego, a także jeżeli w trakcie badania i negocjowania współpracy konieczne jest przekazanie tym osobom działającym na jego zlecenie lub podwykonawcom informacji poufnych dostarczonych przez ET&S lub jego Podmioty powiązane, Odbiorca informacji nałoży na te osoby	**8. Subcontractors, vicarious agents** If the Information receiver intends to use vicarious agents and/or subcontractors within the framework of a cooperation to be concluded and/or within the framework of the execution of a contractual relationship and if it is necessary in the course of the examination and negotiation of the cooperation to provide this vicarious agents and/or subcontractors with confidential information provided by ET&S or its Affiliates he shall impose the confidentiality obligations of this Agreement on the

działające na jego zlecenie lub podwykonawców zobowiązanie do zachowania poufności określone w Umowie i ponosi odpowiedzialność za każde naruszenie tych zobowiązań przez osobę działającą na jego zlecenie lub podwykonawcę.	vicarious agents or subcontractors and shall be liable for any breach of these obligations by the vicarious agent and/or subcontractor.
9. Termin Zobowiązanie do zachowania poufności wynikające z Umowy trwa przez 10 lat po zakończeniu stosunków handlowych między Stronami. W przypadku gdy nie nawiązano stosunków handlowych, obowiązek zachowania poufności wygasa po 10 latach od zakończenia ostatnich negocjacji/rozmów lub zaproszenia do składania ofert. Zobowiązanie do zachowania poufności w przypadku informacji objętych obowiązkiem poufności wynikającym z przepisów prawa obowiązuje bezterminowo.	**9. Term** The confidentiality obligation arising from this Agreement continues for 10 years after the end of the business relationship between the Parties. In the event that no business relationship has been established, the confidentiality obligation ends 10 years after the end of the last negotiations/talks or call for tenders. The obligation to maintain confidentiality in the case of information covered by the obligation of confidentiality resulting from the provisions of law is valid indefinitely.
10. Kara umowna Umowa przyznaje uprawnienia ET&S oraz jego Podmiotom powiązanym, które są w pełni uprawnione do własnych roszczeń. W przypadku naruszenia Umowy, Odbiorca informacji zapłaci uprawnionemu podmiotowi tj. ET&S lub Podmiotowi powiązanemu, karę umowną za każdy przypadek naruszenia, w wysokości 50 000 zł (słownie: pięćdziesiąt tysięcy złotych), oraz zobowiązany będzie do wyrównania szkody przekraczającej tę kwotę na zasadach ogólnych. Roszczenia, o których mowa w niniejszym pkt mogą być kierowane wobec Odbiorcy informacji bezpośrednio przez Podmioty powiązane w przypadku, gdy naruszenie Umowy dotyczy zobowiązania do zachowania poufności w zakresie informacji poufnych tych podmiotów	**10. Contractual penalty** This Agreement entitles ET&S and its Affiliates, which are fully entitled to their own claims. In the event of infringement of this Agreement, the Information receiver shall pay liquidated damages to the entitled company i.e., ET&S or its Affiliate for each case of infringement, in the amount of PLN 50 000 (in writing: fifty thousand zlotys) and damage in excess of such amounts according to general rules. The claims referred to in this point may be directed against the Information receiver directly by the Affiliates if the breach of this Agreement concerns the obligation to maintain confidentiality in the scope of confidential information of these entities.

11. Postanowienia końcowe Umowa wchodzi w życie z dniem złożenia ostatniego z podpisów osób reprezentujących Strony. *[Wariant nr 1] Umowa została sporządzona (i) w formie elektronicznej opatrzonej kwalifikowanymi podpisami elektronicznymi osób reprezentujących ET&S oraz (ii) w formie pisemnej w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron, opatrzonych podpisami osób reprezentujących Odbiorcę informacji / [Wariant nr 2] Umowę sporządzono w formie elektronicznej i opatrzono kwalifikowanymi podpisami elektronicznymi osób reprezentujących Strony.** W przypadku rozbieżności pomiędzy polską a angielską wersją Umowy, obowiązuje wersja polska. Zmiany i uzupełnienia Umowy wymagają dla swej ważności formy pisemnej. Dotyczy to również wszelkich zmian tego wymogu formy pisemnej. Umowa oraz wszystkie prawa i obowiązki w niej określone podlegają prawu polskiemu. Wszelkie spory pomiędzy Stronami będą rozstrzygane przez sąd powszechny właściwy dla siedziby ET&S. Jeżeli poszczególne postanowienia Umowy są lub staną się z mocy prawa nieważne lub nieskuteczne, pozostałe postanowienia pozostają ważne. W takim przypadku Strony zobowiązują się do uzgodnienia w miejsce nieważnego/bezskutecznego postanowienia ważnego/skutecznego postanowienia, które w kontekście Umowy będzie jak najbardziej zbliżone do ekonomicznego znaczenia i celu nieważnego postanowienia. Integralną częścią Umowy są poniższe Załączniki: Załącznik nr 1 – Klasyfikacja informacji poufnych Załącznik nr 2 – Dodatkowe zobowiązania w zakresie bezpieczeństwa informacji ET&S**	**11. Miscellaneous** This Agreement comes into force from upon last signature of persons representing the Parties. *[Option no 1] This Agreement has been drawn up (i) in electronic form signed with qualified electronic signatures of persons representing ET&S and (ii) in writing in two identical copies, one for each of the Parties, signed by persons representing the Information receiver. / [Option no 2] This Agreement has been drawn up in electronic form and signed with qualified electronic signatures of persons representing the Parties.** In case of any discrepancies between the Polish and English version of this Agreement, the Polish version shall prevail. Amendments and supplements to this Agreement must be made in writing in order to be valid. This shall also apply to any amendment of this requirement for written form. This Agreement and all rights and obligations stipulated therein are subject to the law of Poland. Any disputes between the Parties shall be settled by the common court having jurisdiction over registered office of ET&S. Should individual provisions of this Agreement be or become invalid or contain a loophole, the remaining provisions shall remain valid. In this case, the Parties undertake to agree on a valid provision in place of the invalid provision which comes as close as possible to the economically intended meaning and purpose of the invalid provision in the context of the declaration. An integral part of this Agreement are the following annexes: Annex no. 1 - Classification of confidential information

	Annex no. 2 – Additional obligations regarding ET&S's Information security regulations**

ET&S

_____ _____

Data i podpis (y) / Date and signature(s)

Odbiorca informacji/Information receiver

_____ _____

Data i podpis(y) / Date and signature(s)

1.1. Specyfikacje

W kontekście niniejszejszego załącznika, informacja to idea, fakt lub wiedza, która jest rozwijana, zapisywana (lub przechowywana) i wymieniana. Informacja może występować w dwóch różnych formach:

- Informacja analogowa to informacja na papierze,
- informacja cyfrowa to informacja w formie elektronicznej.

Wymagania w niniejszejszym załączniku, MUSZĄ mieć zastosowanie zarówno do informacji analogowych, jak i cyfrowych.

1.2. Obowiązki

ET&S MUSI określić rolę właściciela informacji. Dla każdej informacji MUSI istnieć jeden właściciel informacji.

Z definicji, właściciel informacji jest menedżerem wyższego szczebla w ET&S.
Właściciel informacji jest odpowiedzialny za ochronę informacji w ramach swojego obszaru odpowiedzialności.
Z tego powodu MUSI on:

- sklasyfikować informację (w przypadku zmian w informacji może stać się to konieczne wielokrotnie),
- określić grupę osób, które mają prawo do otrzymania dostępu do informacji,
- przydzielanie sprawdzanie i odbieranie praw dostępu do informacji.

Właściciel informacji ma prawo delegować te zadania. W dalszym ciągu jest on jednak odpowiedzialny za te zadania.

1.2. Poziomy poufności (C)

Prawidłowa klasyfikacja informacji jest WYMAGANA w celu określenia poziomu potrzebnej jej ochrony. Poniższa ilustracja służy jedynie jako krótki przegląd ogólnego schematu klasyfikacji - szczegółowe wymagania są określone w pozostałej części niniejszego dokumentu i MUSZĄ być przestrzegane.

W przypadku klasyfikowania informacji jest to WYMAGANE:

- zasadniczo brać pod uwagę perspektywę przedsiębiorstwa, a nie pojedynczego człowieka,
- rozważenie możliwego wpływu na ET&S lub Grupę ERGO, jeśli dowie się o tym nieupoważniona strona,
- mieć na uwadze, że klauzula pofuności może z czasem wzrosnąć lub zmaleć (np. gdy wzrośnie poziom jej dojrzałości lub informacje wrażliwe zostaną celowo ujawnione),
- w przypadku informacji umożliwiających identyfikację osoby, że uwzględnia się również perspektywę danej osoby.

W kolejnych częściach udokumentowano więcej informacji ogólnych, aby pomóc w zaklasyfikowaniu informacji do jednej z czterech klas poufności C1 - C4.

1.3. Poziom klasyfikacji C1: Publiczne

1.3.1. Opis

Informacje oznaczone klauzulą C1 mogą być udostępniane publicznie w celu zapoznania się z nimi bez żadnych ograniczeń.

1.3.2. Klasyfikacja

Jeśli nie przewiduje się żadnych negatywnych konsekwencji dla firmy lub osób w przypadku upublicznienia lub wycieku tej informacji, jest to wskazówka, że można ją zaklasyfikować jako C1.

1.3.3. Wymagania ochronne

Brak wymagań ochronnych.

1.4. Poziom klasyfikacji C2: Wewnętrzne/ Wyłącznie do użytku wewnętrznego

1.4.1. Opis

Informacji oznaczonych klauzulą C2 NIE WOLNO udostępniać publicznie.

Dostęp może być przyznany dla celów biznesowych wszystkim lub szerszej grupie pracowników, partnerów biznesowych i osób trzecich. Zasada "need-to-know" MUSI być przestrzegana, tzn. MUSI być zapewnione, że dana osoba ma dostęp tylko do informacji potrzebnych do wykonania przydzielonych zadań.

W przypadku informacji umożliwiających identyfikację osoby, dostęp do nich MUSI być ograniczony przynajmniej do ET&S i zakontraktowanego partnera biznesowego (osoby prawnej), chyba że przepisy o ochronie danych osobowych zezwalają na przekazanie tych informacji umożliwiających identyfikację osoby innym spółkom grupy Munich Re, ich partnerom biznesowym lub osobom trzecim.

1.4.2. Klasyfikacja informacji nieosobowych

Jeśli publikacja tej informacji bez ograniczeń dostępu lub warunków wykorzystania zostanie uznana za niewłaściwą, jest to wskazówka, że MUSI ona zostać sklasyfikowana co najmniej jako C2. To samo dotyczy sytuacji, gdy jedna z poniższych konsekwencji mogłaby wystąpić dla firmy w przypadku upublicznienia lub wycieku do nieuprawnionej strony:

- Zgłoszenie do władz, które może zakończyć się drobnym upomnieniem lub grzywną,
- Niski wpływ finansowy lub na reputację (np. lokalne doniesienia prasowe lub niewielkie dyskusje w mediach społecznościowych),
- Niewielki wpływ na ciągłość działania i bezpieczeństwo.

1.4.3. Klasyfikacja informacji umożliwiających identyfikację osób

Wskazówką, że informacja MUSI być sklasyfikowana co najmniej jako C2 jest również to, że w przypadku upublicznienia jej informacji umożliwiających identyfikację osoby lub wycieku tych informacji do nieupoważnionej osoby mogłyby wystąpić następujące konsekwencje: wpływ na prywatność jest niewielki lub umiarkowany.

Zgodnie z definicją Grupy MunichRe, termin "**wpływ na prywatność**" oznacza: fizyczną, materialną lub niematerialną szkodę osób fizycznych, taką jak utrata kontroli nad ich danymi osobowymi lub ograniczenie ich praw, dyskryminację, kradzież tożsamości lub oszustwo, stratę finansową, nieautoryzowane odwrócenie pseudonimizacji, uszczerbek na reputacji, utratę poufności danych osobowych chronionych tajemnicą zawodową lub jakąkolwiek inną znaczącą ekonomiczną lub społeczną szkodę dla osoby fizycznej.

1.4.4. Wymagania ochronne

Następujące wymagania ochronne MUSZĄ być spełnione:

- Weryfikacja czy pracownik, zakontraktowany partner biznesowy lub osoba działająca w imieniu strony trzeciej potrzebuje dostępu do tych informacji (zastosowanie zasady "need-to-know") jest WYMAGANA.
- Działania organizacyjne:
  - W przypadku partnerów biznesowych i osób działających w imieniu strony trzeciej: umowa o zachowaniu poufności jest WYMAGANA, jeżeli dostęp nie może być udzielony na mocy prawa lub na podstawie wskazówek prawnych
  - W przypadku partnerów biznesowych, z którymi nie zawarto umowy: ustne lub pisemne instrukcje są WYMAGANE, aby zachować poufność przekazywanych informacji
- Środki techniczne: stosowanie ogólnie przyjętych środków podstawowych jest WYMAGANE (np. zdefiniowano co najmniej prawa dostępu, wprowadzono system kontroli dostępu i monitoring systemu).

1.5. Poziom klasyfikacji C3: Poufne

1.5.1. Opis

Informacje oznaczone klauzulą C3 są informacjami wrażliwymi. Dlatego wymagana jest zwiększona ochrona przed nieuprawnionym ujawnieniem.

WYMAGANE jest udzielanie dostępu tylko w celach biznesowych i na zasadzie "need-to-know" do ograniczonej grupy osób (np. jednostka organizacyjna, zespół projektowy) składającej się z osób możliwych do zidentyfikowania oraz, na podstawie umowy, do osób zobowiązanych do zachowania poufności, działających w imieniu zakontraktowanego partnera biznesowego.

1.5.2. Klasyfikacja informacji nieosobowych

Jeśli któraś z poniższych konsekwencji mogłaby spotkać firmę w przypadku upublicznienia informacji lub wycieku do nieupoważnionej osoby jest to wskazówka, że informacja MUSI być sklasyfikowana co najmniej jako C3:

- Utrata inwestorów, ważnych klientów, partnerów biznesowych lub pracowników w krytycznych dla biznesu jednostkach
- Procesy sądowe z potencjalnie dużymi karami finansowymi lub nieuchronnymi karami pozbawienia wolności
- Zwiększenie stanu głównych zobowiązań finansowych
- Znaczący uszczerbek na reputacji (np. z powodu publikacji incydentu)
- Duże szkody materialne lub utrata integralności ważnych informacji
- Znaczący wpływ na ciągłość działania i/lub bezpieczeństwo

1.5.3. Klasyfikacja informacji umożliwiających identyfikację osób

Wskazówką, że informacja MUSI być zaklasyfikowana jako C3 jest również to, że którakolwiek z poniższych konsekwencji mogłaby powstać dla danej osoby w przypadku, gdy jej informacje umożliwiające identyfikację osobistą stałyby się publiczne lub wyciekłyby do nieupoważnionej strony:

- wpływ na prywatność jest znaczący lub nawet poważny,
- osobistą utratę lub znaczne ograniczenie swobody woli i działania.

1.5.4. Wymagania ochronne

Następujące wymagania ochronne MUSZĄ być spełnione:

- Sprawdzenie czy pracownik, zakontraktowany partner biznesowy lub osoba działająca w imieniu strony trzeciej potrzebuje dostępu do tych informacji. Należy stosować zasadę "Need-to-know" i unikać wyjątków.
- Należy podjąć organizacyjne środki ochronne, aby zapewnić, że dostęp do odpowiednich danych mają tylko osoby należące do wyraźnie upoważnionych grup:
- W przypadku partnerów biznesowych i osób działających w imieniu strony trzeciej: wymagana jest formalna umowa dotycząca poufności, jeżeli dostęp nie może być udzielony na mocy prawa lub na podstawie opinii prawnej
- Dla partnerów biznesowych niebędących stronami umowy: Pisemne pouczenie o obowiązku zachowania poufności przekazanych informacji
- Środki techniczne: stosowanie ogólnie przyjętych środków podstawowych (np. zdefiniowano co najmniej prawa dostępu, wprowadzono system kontroli dostępu i monitoring systemu).

1.6. Poziom klasyfikacji C4: Ściśle poufne

1.6.1. Opis

Najbardziej restrykcyjną klasą jest C4. Jest ona zarezerwowana dla informacji wymagających najściślejszej ochrony. Informacje oznaczone klauzulą C4 obejmują bardzo wrażliwe informacje umożliwiające identyfikację osób.

WYMAGANE jest udzielanie dostępu tylko osobom wskazanym przez właściciela informacji i wyraźnie wyznaczonym do tego celu, które podpisały umowę o zachowaniu poufności. Wymaga się, aby osoby te miały ważny powód oraz jasną i zrozumiałą potrzebę dostępu do informacji.

1.6.2. Klasyfikacja informacji nieosobowych

Jeżeli którakolwiek z poniższych konsekwencji mogłaby wystąpić dla Grupy ERGO lub ET&S w przypadku niezamierzonego ujawnienia lub poznania informacji przez osoby nieuprawnione, MUSI ona zostać zakwalifikowana jako C4:

- Pojawienie się poważnych przeszkód w realizacji głównych celów biznesowych (np. znaczne i prawie nieodwracalne osłabienie pozycji konkurencyjnej, perspektyw zysku lub pozycji negocjacyjnej w odniesieniu do spraw niezwykle istotnych dla spółki)
- Znaczące konsekwencje prawne lub regulacyjne (np. grzywny), które mogą prowadzić do ogólnej

straty ekonomicznej, wyraźnie widocznej w bilansie danej dziedziny działalności
- Trwały i głęboki uszczerbek dla co najmniej jednej z głównych marek przedsiębiorstwa (uszczerbek na reputacji) z punktu widzenia klienta lub inwestora (np. z powodu utraty danych osobowych osoby publicznej)
- Znaczący wpływ na cele ochrony bezpieczeństwa informacji Grupy ERGO lub ET&S
- Skrajne ryzyko utraty większej liczby kluczowych osób niezbędnych do realizacji głównych celów biznesowych Grupy ERGO lub ET&S
- Poważne zagrożenie dla bezpieczeństwa firmy lub życia i zdrowia

1.6.3. Klasyfikacja informacji umożliwiających identyfikację osób

Wskazówką, że informacja MUSI być sklasyfikowana jako C4 jest również to, że którakolwiek z poniższych konsekwencji mogłaby powstać dla danej osoby w przypadku, gdy jej informacje umożliwiające identyfikację osobistą stałyby się publiczne lub wyciekłyby do nieupoważnionej strony:
- wpływ na prywatność jest niezwykle poważny i nieodwracalny
- poważne ograniczenie/pozbawienie wolności działania i samostanowienia
- poważne zagrożenie dla życia i zdrowia

1.6.4. Wymagania ochronne

Następujące wymagania ochronne MUSZĄ być spełnione:
- Ścisłe sprawdzenie czy otrzymanie danej informacji jest niezbędne dla danej osoby; zasada "need-to-know" MUSI być stosowana bez wyjątku.
- Należy podjąć organizacyjne i techniczne środki ochronne w celu zapewnienia, że odpowiednie dane są dostępne tylko dla osób upoważnionych:
    - Pisemne zobowiązanie do zachowania absolutnej poufności, do przestrzegania odpowiednich dyrektyw i do stosowania dostępnych środków bezpieczeństwa
    - Odbiorca ma zostać poinformowany, we właściwy sposób, o ściśle poufnym charakterze informacji oraz o obowiązkach, jakie na nim ciążą w związku z nimi
    - okresowe przeglądy uprawnień: właściciel informacji musi sprawdzać w rozsądnych odstępach czasu, czy przyznane prawa dostępu są nadal odpowiednie lub konieczne, czy też należy je wycofać
- Środki techniczne: stosowanie ogólnie przyjętych środków podstawowych (np. zdefiniowano co najmniej prawa dostępu, wprowadzono system kontroli dostępu i monitoring systemu).

1.7. Stosowanie klasyfikacji informacji

Wszystkie informacje wytworzone lub zredagowane po dacie publikacji niniejszego dokumentu oraz informacje otrzymane od stron trzecich po tej dacie MUSZĄ być klasyfikowane zgodnie ze schematem określonym w niniejszym dokumencie w miarę możliwości technicznych.

Najbardziej wrażliwa część informacji określa poziom poufności.

Następujące tematy MUSZĄ być uwzględnione w klasyfikacji informacji przedsiębiorstwa (dla każdego poziomu poufności):
- oznakowanie informacyjne (analogowe i cyfrowe),
- przekazywanie informacji (wewnętrznie i zewnętrznie oraz analogowo i cyfrowo) oraz wydawanie

praw dostępu do informacji (cyfrowo),
- przechowywanie (analogowe) i zapisywanie (cyfrowe) informacji,
- rozporządzanie informacją (analogową i cyfrową).

	Atrybuty bezpieczeństwa		
Klasyfikacja informacji	**Poufność**	**Integralność**	**Dostępność**
Publiczne (C1)	Informacja jest ogólnodostępna.	Nieautoryzowana zmiana informacji nie wpływa na możliwość funkcjonowania ET&S ani na zgodność z wymaganiami prawnymi.	Informacja może być dostępna z opóźnieniem wynoszącym więcej niż 2 dni robocze.
Wewnętrzne (C2)	Udostępnienie informacji osobom nieupoważnionym powoduje straty, nie wiąże się z naruszeniem przepisów prawa przez ET&S.	Nieautoryzowana zmiana informacji uniemożliwia poprawną pracę ET&S, ale nie jest związana z naruszeniem przepisów prawnych.	Informacja musi być dostępna z opóźnieniem nie dłuższym niż 2 dni robocze.
Poufne (C3)	Udostępnienie informacji osobom nieupoważnionym powoduje straty i wiąże się z naruszeniem przepisów prawa przez ET&S.	Nieautoryzowana zmiana informacji uniemożliwia poprawną pracę ET&S i skutkuje naruszeniem przepisów prawnych.	Informacja musi być dostępna na żądanie w każdym momencie.
Ściśle poufne (C4)	Udostępnienie informacji osobom nieupoważnionym prowadzi do pojawienia się bardzo poważnych przeszkód w realizacji głównych celów biznesowych oraz do znaczącego naruszenia przepisów prawa przez ET&S.	Nieautoryzowana zmiana informacji uniemożliwia poprawną pracę ET&S i może prowadzić do poważnego zagrożenia dla bezpieczeństwa firmy lub życia i zdrowia.	Informacja musi być dostępna na żądanie w każdym momencie.

1. Specifications

In the context of this Annex, an information is an idea, fact, or knowledge, that is developed, recorded (or saved) and exchanged. Information can be existent in two different forms:

- analogue information is information on paper,
- digital information is information in electronic form.

The requirements in this Annex, MUST apply for analogue as well as for digital information.

1.1 Responsibilities

ET&S MUST establish the role of the information owner. For each information one information owner MUST exist.

By definition, an information owner is an ET&S senior manager.
An information owner is responsible for the protection of information within his area of responsibility. For this reason, he MUST:

- classify the information (in the case of changes in the information, this can become necessary repeatedly),
- define the group of people who are allowed to receive access to the information,
- allocate check and revoke the access rights for information.

The information owner is allowed to delegate these tasks. He continues, however, to be responsible for the tasks.

1.2 Confidentiality levels (C)

1.1

Correct classification of information is REQUIRED to determine the level of its protection needs. The following illustration only serves as a short overview of the general classification scheme – detailed requirements are specified in the remainder of this document and MUST be adhered to.

When classifying information, it is REQUIRED:

- to principally take the company's perspective into account rather than that of an individual,
- to consider the possible impact for the ET&S or for ERGO Group, if an unauthorized party becomes aware of it,
- to bear in mind that the classification may increase or decrease over time (e.g., when the level of its maturity rises or sensitive information is released on purpose),
- for personally identifiable information, that the relevant individual's perspective is also taken into account.

In the following sections, more background information is documented in order to help classify information in one of the four confidentiality classes C1 – C4.

1.3 Classification Level C1: Unrestricted/Public

1.3.1 Description

C1-classified information can be made publicly available for perusal with no restrictions.

1.3.2 Classification

If no negative consequences for the company or individuals are expected when this information becomes public or is leaked, this is an indication that it can be classified as C1.

1.3.3 Protective requirements

None protective requirements.

1.4 Classification Level C2: Internal/For internal use only

1.4.1 Description

C2-classified information MUST NOT be made accessible to the public.

Access can be granted for business-related purposes to all or a wider group of employees, business partners and third parties. The ”need-to-know“ principle MUST be adhered to, i.e., it MUST be ensured that a person only has access to the information needed to fulfil the assigned tasks.

For personally identifiable information, at least access to it MUST be restricted to ET&S and to contracted business partner (legal entity), unless data protection laws allow the transfer of this personally identifiable information to other Munich Re Group companies, their business partners or third parties.

1.4.2 Classification of non-personal information

If the publication of this information without access restrictions or conditions of use is considered inappropriate, it is an indication that it MUST be classified at least as C2. The same applies if one of the following consequences could occur for the company if it becomes public or is leaked to an unauthorized party:

- Report to authorities that could result in a minor rebuke or fine,
- Low financial or reputational impact (e.g., local press reports or minor social media discussion),
- Negligible impact on business continuity and safety.

1.4.3 Classification of personally identifiable information

An indication that the information MUST be classified at least as C2 also is, if the following consequence could arise for the relevant individual in case his or her personally identifiable information would become public or would be leaked to an unauthorized party: impact on privacy is small or moderate.

In alignment with the MunichRe Group definition, the term "**impact on privacy**" means: Physical, material or non-material damage to natural persons, such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage to the natural person.

1.4.4 Protective requirements

The following protective requirements MUST be met:

- Verification of whether the employee, the contracted business partner or the person acting on behalf of a third party needs access to this information (application of the "need-to-know" principle) is REQUIRED.
- Organizational measures:
    - For contracted business partners and persons acting on behalf of a third party: confidentiality agreement is REQUIRED where access is not to be granted by law or on the basis of regulatory advice
    - For non-contracted business partners: verbal or written instruction is REQUIRED to keep the information provided confidential
- Technical measures: application of generally accepted basic measures is REQUIRED (e.g., at least access rights are defined, an access control system and system monitoring are in place).

1.5 Classification level C3: Confidential

1.5.1 Description

C3-classified information is sensitive information. Therefore increased protection against un-authorized disclosure is REQUIRED.

It is REQUIRED to grant access only for business-related purposes and on a "need-to-know" basis to a limited group of people (e.g. organizational unit, project team) consisting of identifiable persons and, contractually, to non-disclosure-obligated persons acting on behalf of a contracted business partner.

1.5.2 Classification of non-personal information

If any of the following consequences could arise for the company if information becomes public or is leaked to an unauthorized
party, this is an indication that the information MUST be classified at least as C3:

- Loss of investors, important clients, business partners or employees in business-critical units
- Lawsuits with potentially major financial fines or imminent terms of imprisonment
- Increment of major financial liabilities
- Significant reputational damage (e.g. due to publication of the incident)
- High material damage or loss of integrity of important information
- Significant impact on business continuity and/or safety

1.5.3 Classification of personally identifiable information

An indication that the information MUST be classified as C3 also is, if any of the following consequences could arise for the relevant individual in case his or her personally identifiable information would become public or would be leaked to an unauthorized party:

- impact on privacy is significant or even serious,
- personal loss or significant restriction of freedom of will and action.

1.5.4 Protective requirements

The following protective requirements MUST be met:

- Verification of whether the employee, the contracted business partner or the person acting on behalf of a third party needs access to this information. The ”Need-to-know“ principle is to be applied and exceptions are to be avoided.
- Organizational protective measures are to be taken to ensure that the relevant data can only be accessed by those belonging to explicitly authorized groups:
- For contracted business partners and persons acting on behalf of a third party: formal agreement regarding confidentiality required where access is not to be granted by law or on basis of regulatory advice
- For non-contracted business partners: Written instruction to be obliged to keep the information provided confidential
- Technical measures: application of generally accepted basic measures (e.g., at least access rights are defined, an access control system and system monitoring are in place).

1.6 Classification level C4: Strictly Confidential

1.6.1 Description

The most restrictive class is C4. It is reserved for information requiring the strictest protection. C4-classified information includes very sensitive personally identifiable information.

It is REQUIRED to grant access only to persons named by the information owner and expressly designated for the purpose who have signed a non-disclosure agreement. It is REQUIRED for these persons to have an important reason and a clear and understandable need to access the information.

1.6.2 Classification of non-personal information

If any of the following consequences could arise for the ERGO Group or ET&S in the event of unintentional disclosure or knowledge of the information by unauthorized individuals, it MUST be classified as C4:

- Emergence of serious obstacles in achieving its main business objectives (e.g. significant and nearly irreversible weakening of its competitive position, profit prospects or negotiating position in relation to matters of extremely importance to the company)
- Significant legal or regulatory consequences (e.g. fines), which may lead to an overall economic loss that is clearly visible in the balance sheet of the business field
- Sustained and profound damage to at least one of the business field’s core brands (reputational damage) from the client's or investor's point of view (e.g. because of the loss

of personal data of a person of public interest)
- Significant impact on information security protection goals of the ERGO Group or ET&S
- Extreme risk of losing a larger number of key individuals required to achieve main business objectives of the ERGO Group or ET&S
- Serious threat to corporate security or life and limb

1.6.3 Classification of personal identifiable information

An indication that the information MUST be classified as C4 also is, if any of the following consequences could arise for the relevant individual in case his or her personally identifiable information would become public or would be leaked to an unauthorized party:

- impact on privacy is extremely serious and irreversible
- severe restriction/deprivation of freedom of action and self-determination
- acute threat for life and limb

1.6.4 Protective requirements

The following protective requirements MUST be met:

- Strict verification of whether it is indispensable for the person to receive the information in question; the ”need-to-know“ principle MUST be applied without exception.
- Organizational and technical protective measures are to be taken to ensure that the relevant data is only accessible to authorized persons:
    - Written commitment to maintain absolute confidentiality, to comply with the relevant directives and to apply the available security measures
    - The recipient is to be made aware, in an appropriate manner, of the strict confidential nature of the information and of the obligations incumbent upon him in connection therewith
    - Recurrent entitlement reviews: the information owner has to check at reasonable intervals whether the access rights granted are still appropriate or necessary or whether they need to be withdrawn
- Technical measures: application of generally accepted basic measures (e.g. at least access rights are defined, an access control system and system monitoring are in place).

1.7 Use of the information classification

All information generated or edited after the date of publication of this document and information received from third parties since that date MUST be classified in accordance with the scheme set out in this document as far as technically possible.

The most sensitive part of an information determines the confidentiality level.

The following topics MUST be covered in the information classification of the company (for each level of confidentiality):

- information labelling (analogue and digital),
- forwarding information (internally and externally as well as analogue and digital) and issuing of access rights for information (digital),

- storing (analogue) and saving (digital) information,
- disposing of information (analogue and digital).

	Security attributes		
Information classification	**Confidentiality**	**Integrity**	**Availability**
Public (C1)	The information is publicly available.	Unauthorised changes to the information do not affect ET&S's ability to function or compliance with legal requirements.	Information may be available with a delay of more than 2 working days.
Internal (C2)	The release of information to unauthorised persons results in losses and does not involve a breach of the law by ET&S.	Unauthorised alteration of information prevents the correct operation of ET&S, but is not associated with a legal violation.	The information must be available with a delay of no more than 2 working days.
Confidential (C3)	The release of information to unauthorised persons causes losses and involves a breach of the law by ET&S.	Unauthorised alteration of the information prevents the correct operation of the ET& S and results in a breach of the law.	Information must be available on request at any time.
Strictly confidential (C4)	The release of information to unauthorised persons leads to the appearance of very serious impediments to the achievement of core business objectives and a significant breach of the law by ET&S.	Unauthorised alteration of information prevents ET&S from working properly and can lead to serious risks to company safety or life and health.	Information must be available on request at any time.