|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | On behalf of |  | processed by the | |  |  | softgarden e-recruiting GmbH  Tauentzien Strasse 14  10789 Berlin, Germany | | - hereafter referred to as the "**Principal**" - |  | - hereafter referred to as the "**Contractor**" - |   collectively referred to hereafter as **Contract Partners**.  **Preamble**  This Data Protection Contract shall regulate the protection of personal data when processed on commission.  If a controller (Principal) has personal data processed by another controller (Contractor), Art. 28 of the General Data Protection Regulation requires the conclusion of a written contract for the commissioned data processing. In addition to storage, edits, transfers, blocking and deletion, data processing also includes the providing of data for third-party inspections or retrieval.  The Principal shall be responsible for processing the personal data in accordance with data protection regulations. Under Art. 29 of the General Data Protection Regulation, the Contractor may only process the data if directed to do so by the Principal. In case of violations by the Contractor, e.g., by determining purposes of the processing himself, under Art. 28(10) of the General Data Protection Regulation, the Contractor will become the controller for the data subject.  Therefore, the Contract Parties shall agree to the following: Object of this Order The object of the order shall follow from the agreement described in **Annex 1**. This agreement, hereafter referred to as the "main agreement" shall be referred to hereafter. Order Content Specification  1. The specification of the order contents, the data and of the circle of persons affected by the data collection, processing or use can be found in **Annex 1** to this Data Protection Contract. 2. The data shall only be processed and used in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another state party to the EEA Agreement. Any outsourcing to a third country shall require the Principal's prior written permission and may only be performed if the special requirements of Art. 44 to Art. 50 of the General Data Protection Regulation are fulfilled.  Technical and Organizational Measures  1. Before the processing, the Contractor must document the implementation of the technical and organizational described prior to the awarding of the order, especially regarding the specific performance of the order, and submit the documentation to the Principal for review. Following the Principal's acceptance, the documented measures shall form the basis of the order. If the review/an audit by the Principal finds need for adjustments, these must be implemented mutually. 2. The measures to be taken must ensure the confidentiality, integrity, availability and resilience of the systems and services for the processing of personal data; measures for quickly restoring the availability of and access to personal data in case of physical or technical incidents and measures that guarantee the effectiveness of these measures through regular reviews, assessments and evaluations (for specifics, see **Annex 2**). 3. The technical and organizational measures are subject to technical progress and developments. Therefore, the Contractor may implement adequate alternative measures. However, the security level of the specified measures must be maintained. Significant changes must be documented and provided to the Principal on request. 4. The Principal may, at any time, review or have the concluded agreement reviewed by a competent third party regarding the technical and organizational measures.  Rights of the data subject  1. The Contractor may only rectify, erase or block the data processed on commission in accordance with the Principal's directives. If a data subject contacts the Contractor directly for exercising the their rights as of Chapter III GDPR, the Contractor must forward this request to the Principal without undue delay. 2. If covered by the service scope, execution of a request in order to fulfill the rights of a data subject must be ensured directly by the Contractor in accordance with documented directives of the Principal. 3. Any actions under Section 4 of this Contract must be recorded and submitted to the Principal in writing.  Duties of the Contractor The Contractor shall have the following duties:   1. If required under Art. 37 *et seq*. of the General Data Protection Regulation, the appointment of a data protection officer whose contact details must be provided to the Principal to allow the Principal contact the data protection officer directly (**Annex 1**). 2. The duty to subject all persons who may access the Principal's data for the order to confidentiality obligations (Art. 28(3) Sentence 2 Letter b of the General Data Protection Regulation) and to inform these persons about the data protection regulations of the order and about the subjection to directives and the purposes for the processing. 3. The duty to implement and maintain any technical and organizational measures required for this order in accordance with Art. 32 of the General Data Protection Regulation (see Art. 28(3) Sentence 2 Letter c of the General Data Protection Regulation). 4. The duty to take any required technical and organizational measures to allow the Principal to comply with the data subject rights under Chapter III of the General Data Protection Regulation (information, access, rectification and erasure, data portability and to object and, in individual cases, automated decision-making) at any time during the legally required period (see Art. 28(3) Sentence 2 Letter e of the General Data Protection Regulation). For this, the Contractor must provide any required information to the Principal. This requires the Principal to have issued  a corresponding written directive to the Contractor and this assistance to not violate the Contractor's non-disclosure obligations to third parties. The Contractor shall reserve the right to pass on any costs incurred thereby to the Principal separately. 5. The duty to assist the Principal to comply with the obligations under Art. 32 to Art. 36 of the General Data Protection Regulation (data security measures, reporting infringements on the protection of personal data to supervisory authorities, notification in case of violations of the protection of personal data of data subjects, data protection impact assessments, prior consultation) (see Art. 28(3) Sentence 2 Letter f of the General Data Protection Regulation). 6. The duty to inform the Principal without undue delay about any control actions and measures by supervisory authorities (see Art. 31 & Art. 51 *et seq*. of the General Data Protection Regulation). This shall also apply if the competent authorities under Art. 83 & Art. 84 of the General Data Protection Regulation investigate the Contractor. 7. The Contractor must state in writing the intended location(s) of his offices or of the Principal's computer centers used for using the Principal's data for the order (**Annex 1**). Contractor informs the principal without delay of any change or new signing in regard to a subcontractor. Principal is allowed to raise an objection against any of these changes (Art. 28 Sec. 2 GDPR). Such objection may not be issued without significant reason (e.g. (planed) involvement of a principal´s competitor, former known data privacy violations). Such notice in regard to a change in subcontractors has to be issued within two weeks prior to the change of subcontractors to the principal´s instructor. If principal does not issue any objection within two weeks after notice, the principal´s permission is deemed as given. The Contractor must ensure that third-party access to the Principal's data processed at the Contractor's locations stated in Annex 1 is excluded. 8. The Contractor may state the person(s) authorized to receive the Principal's directives to the Principal. Persons of the Contractor who may issue directives must be documented in **Annex 1**. 9. In case of a data transfer to an unsafe third country, the transfer must be made permissible using the legal options provided by the European Commission.  Subcontractual Relationships The inclusion of subcontractors in the processing or use of the Principal's personal data shall be permitted if the following requirements are met:   1. The inclusion of subcontractors who directly use the Principal's data on the Contractor's behalf is documented in writing in **Annex 1**. For the named subcontractors within Annex 1 Principal´s consent is deemed as given by singing of this contract. Use in the sense of this Contract includes read access to personal data and any further activities. 2. Agreements concluded between the Contractor and subcontractors must correspond to the data protection regulations of the Contractual relationship between the Principal and the Contractor. Proof of the conformity of such agreements must be submitted to the Principal in writing on request. 3. Contractor informs the principal without delay of any change or new signing in regard to a subcontractor. Principal is allowed to raise an objection against any of these changes (Art. 28 Sec. 2 GDPR). Such objection may not be issued without significant reason (e.g. (planed) involvement of a principal´s competitor, former known data privacy violations). Such notice in regard to a change in subcontractors has to be issued within two weeks prior to the change of subcontractors to the principal´s instructor. If principal does not issue any objection within two weeks after notice, the principal´s permission is deemed as given. If a subcontractor uses this data in an unsafe third country, the legal means provided by the European Commission for ensuring an adequate level of data protection must be applied.   Third-party services utilized by the Contractor as ancillary services for assistance with order performance shall not be considered sub-contractual relationships in the sense of this regulation. For example, this shall include cleaning services, pure telecommunications services that do not specifically relate to services performed by the Contractor for the Principal, mailing or courier services, transport services or security services. The Contractor must ensure that appropriate precautions and technical and organizational measures are taken to guarantee the protection of personal data, including for ancillary services. IT system maintenance and inspection shall represent sub-contractual relationships requiring permission if IT systems needed for the performance of services for the Principal are involved. Control Rights of the Principal  1. The Principal shall have the right to perform order controls at his own expense, during regular business hours in consultation with the Contractor without disrupting business operations or to have such order controls performed by inspectors to be appointed in individual cases if they are not competitors of the Contractors and if the Contractor has no legitimate objections. On request, the Contractor shall provide any information and corresponding proof to the Principal required for fulfilling his order control obligations. 2. For the Principal's control obligations under Art. 28(1) of the General Data Protection Regulation prior to data processing and during the duration of the order, the Contractor shall ensure that the Principal can review compliance with the implemented technical and organizational measures. For this, the Contractor shall demonstrate the implementation of the technical and organizational measures in accordance with Art. 32 of the General Data Protection Regulation to the Principal on request. Proof of the implementation of such measures that only concern the respective order may also be provided through current certificates, reports or excerpts thereof (e.g., from an auditor, audit, data protection officer, IT security department, data protection auditors, quality auditors) or suitable certification for an IT security or data protection audit (e.g., under BSI IT-Grundschutz) or through adherence to an approved code of conduct (so-called BCR). The Contractor shall reserve the right to pass on any costs incurred thereby to the Principal separately. 3. If the Principal discovers errors or irregularities regarding data protection regulations, the Principal shall notify the Contractor about this without undue delay.  Contractor Violation Reports  1. The Contractor shall notify the Principal if the Contractor or his employees violate any data protection regulations applicable to the Principal's data or to the specifications of the order. 2. It is known that under Art. 33 of the General Data Protection Regulation, third parties may have to be notified if personal data concerning them may have been lost or transmitted unlawfully or if knowledge of the personal data may have been obtained unlawfully. Therefore, such incidents must be reported to the Principal without undue delay, irrespective of their cause. This shall also apply in case of severe operational disruptions and suspicions of other violations of personal data protection regulations or of other irregularities when handling the Principal's personal data. The Contractor must in consultation with the Principal, take appropriate measures for securing the data and reducing any disadvantageous consequences for the data subjects. The Contractor must assist the Principal with the fulfillment of any obligations under Art. 33 or Art. 34 of the General Data Protection Regulation to which the Principal may be subject.  Principal's Authority to Issue Directives  1. Data shall be treated exclusively in accordance with the concluded agreements and the Principal's directives (see Art. 28(3) Sentence 2 Letter a) of the General Data Protection Regulation). As part of the order description under this Contract, the Principal shall reserve an extensive right to issue directives on the type, scope and procedure for data processing which may be further specified through individual directives. Changes to the processing object and procedural changes must be jointly coordinated and documented in writing. The Contractor may only provide information to third parties or data subjects with the Principal's prior written permission. 2. The Principal shall confirm any oral directives in writing or by email (in text form) without undue delay. The Contractor may not use the data for any other purposes and may especially not provide the data to third parties. Copies or duplicates of the data may not be created without the Principal's knowledge. However, this shall not apply to backup copies required for ensuring orderly data processing or to data necessary for compliance with legal storage obligations. 3. The Principal may appoint persons with the authority to issue directives. If the Contractor processes sensitive data for the Principal, the Principal shall directly appoint the persons with the authority to issue directives who must legitimize themselves when exercising their authority. The Principal's persons with the authority to issue directives shall be documented in **Annex 1**. Any changes to the Principal's or Contractor's persons with the authority to issue directives shall be reported in writing and recorded in **Annex 1**. 4. The Contractor must notify the Principal in accordance with Art. 28(3) Sentence 3 of the General Data Protection Regulation without undue delay if the Contractor believes that a directive of the Principal violates data protection regulations. The Contractor may suspend the performance of the respective directive until the directive is confirmed or changed by the Principal.  Data Deletion and Data Carrier Returning When Activities End  1. After the completion of the processing or after this Contract ends at the latest, the Contractor must hand over any documents, processing or usage results, personal data copied or produced for service performance and any other confidential data related to the order and in the Contractor's possession to the Principal or delete or destroy them in coordination with the Principal and in compliance with data protection regulations. Test and scrap material must be destroyed in compliance with data protection regulations or handed over to the Principal without undue delay. This obligation shall apply to the same measure to any commissioned subcontractors. Data and copies thereof required for the fulfillment of liability and guarantee claims shall remain unaffected. 2. The Contractor must save any documentation used for the order or for orderly data processing or that may not be deleted for legal reasons, e.g., due to storage obligations, after this Contract ends for the respective storage periods and must be safely deleted thereafter. The Principal must be  notified about the type and scope of the data saved under Subsection (1) or (2). The Contractor may hand over these data to the Principal for his relief when this Contract ends. 3. The Contractor must confirm the safe deletion or safe destruction of any documents in his possession to the Principal in writing after this Contract ends.  Contract Duration and Termination  1. The Contractual relationship shall enter into effect upon being signed by both Contract Partners and shall be concluded indefinitely, at least for the same duration as the main contract's duration. Ordinary termination rights shall correspond to those under the main agreement. 2. To supplement the main agreement, it shall be regulated that violations of legal or Contractual data protection regulations by the Contractor shall represent a compelling reason for exercising the extraordinary termination rights reserved under the main agreement for the Principal. Accordingly, the Principal may terminate the main agreement for a compelling reason without notice. 3. If the basis for Contract fulfillment is significantly changed or removed due to legal or rights changes or intervention or other measures by supervisory authorities, both parties shall be entitled to Contractual adjustments to the new circumstances to the extent possible and reasonable for both parties. If Contractual adjustments are not possible or reasonable for a party, this shall represent a compelling reason for both parties for termination without notice. Subsection (2) shall remain unaffected.  Final Provisions  1. Should a regulation of this Contract be or become invalid, the validity of the remainder of the Contract shall remain affected. In such cases, a regulation that most closely approximates the intent of the invalid regulation shall be agreed between the parties. 2. Changes or additions to this Contract, individual agreements or any parts thereof must be issued in written form. This shall also apply to any waiver of this written form requirement. 3. The defense of rights of retention in the sense of Section 273 of the German Civil Code [Bürgerliches Gesetzbuch, BGB] for the processed data and according data carriers shall be excluded. 4. The legal relationships of the Contract Partners shall be governed by the law of the Federal Republic of Germany under exclusion of the UN sales convention and under exclusion of any regulations under German law that refer to a legal system other than the German legal system. 5. For any disputes under or in relation to this Contract, the place of jurisdiction of the main  agreement shall apply as far as permissible. 6. If regulations of this Contract apply beyond the Contractual duration, these regulations shall  remain effective even after the Contract ends. 7. The included Annexes shall be essential parts of this Contract.   **Annex 1: Commissioned Data Processing Contract**  **Annex 2: Technical and Organizational Measure Determination Agreement**   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  | Place, Date |  | Place, Date | |  |  |  |  | |  | Principal  Name / Signature / Company Stamp |  | Contractor  Mathias Heese / Managing Director  Martin Behrend / VP Finance  Name / Signature / Company Stamp | | |  |  |  | | --- | --- | --- | | Na zlecenie |  | opracował | |  |  | softgarden e-recruiting GmbH  Tauentzienstraße 14  10789 Berlin | | - dalej zwana „**Zleceniodawcą**” |  | - dalej zwana „**Zleceniobiorcą**” |   wspólnie nazywane **stronami umowy**.  **Preambuła**  Niniejsza umowa o ochronie danych osobowych reguluje ochronę danych osobowych podczas przetwarzania danych na zlecenie.  Jeżeli administrator (Zleceniodawca) zleca przetwarzanie danych osobowych innemu podmiotowi przetwarzającemu (Zleceniobiorca), strony muszą zawrzeć umowę w formie pisemnej o przetwarzanie danych zgodnie z art. 28 RODO. Do przetwarzania danych poza zapisywaniem, zmianą, przekazywaniem i usuwaniem zalicza się również udostępnianie danych do wglądu lub pobrania przez osoby trzecie.  Zleceniodawca ponosi odpowiedzialność za przetwarzanie danych osobowych zgodnie z prawem ochrony danych. Według art. 29 RODO Zleceniobiorca przetwarza dane wyłącznie na polecenie Zleceniodawcy. Jeżeli Zleceniobiorca naruszy ten obowiązek, przykładowo samemu określając cele przetwarzania, zgodnie z art. 28 ust. 10 RODO uznaje się go za administratora.  Z tego względu strony postanawiają jak poniżej: Przedmiot zlecenia Przedmiot zlecenia opisany jest w umowie określonej w **Załączniku 1**. Wskazuje się na tę umowę, nazywaną dalej „umową główną”. Sprecyzowanie treści zlecenia  1. Sprecyzowanie treści zlecenia, danych i zakresu pobierania, przetwarzania i użytkowania danych osób, których dotyczą, znajduje się w **Załączniku 1** do niniejszej umowy o ochronie danych osobowych. 2. Dane są przetwarzane i użytkowane wyłącznie na terenie Republiki Federalnej Niemiec w kraju członkowskim Unii Europejskiej lub w innym państwie stronie porozumienia o Europejskim Obszarze Gospodarczym. Ewentualne przeniesienie do kraju trzeciego wymaga uprzedniej zgody Zleceniodawcy i może nastąpić wyłącznie wtedy, jeżeli spełnione są warunki specjalne, wynikające z art. 44 do 50 RODO.  Środki techniczno-organizacyjne  1. Przed rozpoczęciem przetwarzania Zleceniobiorca dokumentuje wdrożenie środków techniczno-organizacyjnych określonych przed udzieleniem zlecenia, przede wszystkim dotyczących konkretnego wykonania zlecenia i przedkłada Zleceniodawcy do sprawdzenia. Po zaakceptowaniu przez Zleceniodawcę udokumentowane środki będą podstawą zlecenia. Jeżeli kontrola/audyt Zleceniodawcy wykaże potrzebę dostosowania środków, należy ją wspólnie wdrożyć.      1. Zasadniczo środki, które należy podjąć, to działania gwarantujące poufność, spójność, dostępność i obciążalność systemów oraz usług w związku z przetwarzaniem danych osobowych; środki, które natychmiastowo przywracają dostępność danych osobowych oraz dostęp do nich w przypadku zdarzenia fizycznego lub technicznego oraz środki, które poprzez regularne kontrole, analizy i oceny gwarantują skuteczność działań (szczegóły w **Załączniku 2**). 2. Środki techniczno-organizacyjne podlegają postępowi technicznemu oraz dalszemu rozwojowi. Zleceniobiorca może wdrażać odpowiednie środki alternatywne, o ile dostanie na to zgodę. Przy tym nie mogą one posiadać niższego poziomu bezpieczeństwa niż ustalone środki. Należy dokumentować istotne zmiany i na żądanie udostępniać je Zleceniodawcy. 3. Zleceniodawca jest w każdej chwili upoważniony do sprawdzenia podjętych postanowień w zakresie środków techniczno-organizacyjnych lub zlecić ich sprawdzenie osobie trzeciej.  Prawa osób, których dane dotyczą  1. Zleceniobiorca koryguje, usuwa lub blokuje dane, które są przetwarzane w ramach zlecenia, wyłącznie na polecenie Zleceniodawcy. Jeżeli osoba, której dane dotyczą, zwróci się bezpośrednio do Zleceniobiorcy w celu ochrony praw zgodnie z rozdziałem III RODO, Zleceniobiorca niezwłocznie przekaże tę prośbę Zleceniodawcy. 2. Zleceniobiorca bezpośrednio na udokumentowane polecenie Zleceniodawcy gwarantuje przetworzenie zapytania osoby, której dane dotyczą, w zakresie ochrony jej danych, o ile obejmuje to zakres usług. 3. Wszelkie działania zgodnie z postanowieniem § 4 niniejszej umowy należy przekazywać w formie pisemnej Zleceniodawcy i zachowywać.  Obowiązki Zleceniobiorcy Zleceniobiorca ma następujące obowiązki:   1. Jeżeli zgodnie z art. 37 i nast. RODO określono ustawowo obowiązek wyznaczenia inspektora danych osobowych. Należy przekazać jego dane kontaktowe Zleceniodawcy w celu umożliwienia bezpośredniego kontaktu (**Załącznik 1**). 2. Zobowiązanie wszystkich osób, które zgodnie ze zleceniem mogą mieć dostęp do danych osobowych Zleceniodawcy (art. 28 ust. 3 str. 2 lit. b) RODO) do zachowania poufności oraz obowiązek pouczenia o wynikających ze zlecenia szczególnych zobowiązaniach w zakresie ochrony danych i aktualnych poleceniach lub celach. 3. Obowiązek wdrożenia i stosowania się do wszystkich wymaganych w ramach zlecenia środków techniczno-organizacyjnych zgodnie z art. 32 RODO (zob. art. 28 ust. 3 str. 2 lit. c) RODO). 4. Obowiązek podejmowania wszystkich wymaganych środków techniczno-organizacyjnych, aby Zleceniodawca mógł w każdej chwili zaspokoić prawa osób, których dane dotyczą, zgodnie z rozdziałem III RODO (informacja; udzielanie odpowiedzi; sprostowanie i usuwanie danych; przenoszenie danych; prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach) w ustawowo określonych terminach (zob. art. 28 ust. 3 str. 2 lit. e) RODO). W tym celu Zleceniobiorca przekazuje Zleceniodawcy wszystkie niezbędne informacje. Przyjmuje się, że Zleceniodawca zlecił to pisemnie Zleceniobiorcy, a pomoc nie narusza obowiązków Zleceniobiorcy do zachowania tajemnicy względem osób trzecich. Zleceniobiorca zastrzega sobie prawo do obciążenia Zleceniodawcy związanymi z tym kosztami na oddzielnej fakturze. 5. Obowiązek wspierania Zleceniodawcy w zakresie stosowania się do zobowiązań określonych w art. 32 do 36 RODO (bezpieczeństwo przetwarzania; zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu; zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych; ocena skutków dla ochrony danych; uprzednia konsultacja) (zob. art. 28 ust. 3 str. 2 lit. f) RODO). 6. Obowiązek niezwłocznego informowania Zleceniodawcy o działaniach kontrolnych i środkach rady nadzorczej (zob. art. 31, 51 i nast. RODO). Obowiązuje to również w przypadku, gdy zgodnie z art. 83, 84 RODO organ właściwy prowadzi dochodzenie u Zleceniobiorcy. 7. Zleceniobiorca wyznaczy pisemnie Zleceniodawcy miejsce/miejsca w celu korzystania z danych Zleceniodawcy w ramach stosunku umownego na obszarach jego działalności lub centrów danych przed zawarciem umowy (**Załącznik 1**). Zleceniobiorca niezwłocznie informuje Zleceniodawcę o każdej planowanej zmianie w zakresie dodania nowego lub zmiany dotychczasowego miejsca przetwarzania, przy czym Zleceniodawca ma możliwość sprzeciwić się takiej zmianie (art. 28 ust. 2 zdanie 2 RODO). Sprzeciwu nie należy zgłaszać bez ważnego uzasadnienia (np. zatrudnianie konkurencji Zleceniodawcy lub wcześniejsze naruszenia ochrony danych przez podwykonawcę). Informację o planowanej zmianie podwykonawcy należy przekazać osobie upoważnionej przez Zleceniodawcę do wydawania poleceń. Jeżeli w ciągu dwóch tygodni od momentu zapoznania się z zawiadomieniem o zmianach Zleceniodawca nie sprzeciwi się planowanej zmianie w podanym wyżej sensie, uznaje się, że zgoda została udzielona. Zleceniobiorca zapewnia, że osoby trzecie nie mają dostępu fizycznego do danych Zleceniodawcy, które są przetwarzane w siedzibie/siedzibach podanej/podanych w Załączniku 1. 8. Zleceniobiorca może wyznaczyć osobę/-y dla Zleceniodawcy, która/-e jest/są upoważniona/-e do otrzymywania poleceń od Zleceniodawcy. Osoby upoważnione przez Zleceniobiorcę do otrzymywania poleceń podane są w **Załączniku 1**. 9. Jeżeli dane przenoszone są do niezabezpieczonego państwa trzeciego, transfer należy przeprowadzić przy użyciu dopuszczonych czynności prawnych zatwierdzonych przez Komisję UE.  Stosunki z podwykonawcami Wyraża się zgodę na przetwarzanie lub użytkowanie danych osobowych Zleceniodawcy przez podwykonawców, jeżeli zostaną spełnione poniższe warunki:   1. W **Załączniku 1** należy udokumentować włączenie podwykonawców, którzy będą bezpośrednio korzystać z danych Zleceniodawcy na rzecz Zleceniobiorcy. Dla podwykonawców podanych w Załączniku 1 podczas zawierania obowiązuje zgoda na wykonywanie czynności zgodnie z ustępem 1. Korzystanie w rozumieniu niniejszej umowy obejmuje również dostęp do odczytu danych osobowych oraz związane z tym czynności. 2. Zleceniobiorca tak sformułuje porozumienia umowne z podwykonawcami, aby były one zgodne z postanowieniami w zakresie danych osobowych pomiędzy Zleceniodawcą, a Zleceniobiorcą. Zleceniobiorca przedłoży na żądanie Zleceniodawcy potwierdzenie zgodności w formie pisemnej. 3. Zleceniobiorca niezwłocznie informuje Zleceniodawcę o każdej planowanej zmianie w zakresie dodania nowego lub zastąpienia dotychczasowego podwykonawcy, aby dać Zleceniodawcy możliwość sprzeciwienia się takim zmianom (art. 28 ust. 2 zdanie 2 RODO). Sprzeciwu nie należy zgłaszać bez ważnego uzasadnienia (np. zatrudnianie konkurencji Zleceniodawcy lub wcześniejsze naruszenia ochrony danych przez podwykonawcę). Informację o planowanej zmianie podwykonawcy należy przekazać osobie upoważnionej przez Zleceniodawcę do wydawania poleceń. Jeżeli w ciągu dwóch tygodni od momentu zapoznania się z zawiadomieniem o zmianach Zleceniodawca nie sprzeciwi się planowanej zmianie w podanym wyżej sensie, uznaje się, że zgoda została udzielona. Jeżeli podwykonawca korzysta z danych w niezabezpieczonym państwie trzecim, należy stosować się do środków prawnych określonych przez Komisję UE środków prawnych w zakresie zapewnienia poziomu ochrony danych.   W rozumieniu niniejszego postanowienia do stosunków podwykonawczych nie zalicza się takich usług, z których Zleceniobiorca korzysta za pośrednictwem osób trzecich jako usługa dodatkowa służąca wsparciu wykonania zlecenia. Przykładowo zaliczają się do tego usługi w zakresie sprzątania, typowe usługi telekomunikacyjne bez konkretnego odniesienia do usług, które Zleceniobiorca świadczy względem Zleceniodawcy, usługi pocztowe i kurierskie, usługi transportowe, usługi dozorowania. Zleceniobiorca równocześnie jest zobowiązany zapewnić, również w przypadku usług dodatkowych świadczonych przez osoby trzecie, że podjęto stosowane działania i środki techniczno-organizacyjne w celu zapewnienia ochrony danych osobowych. Konserwacja i kontrola systemów IT zaliczają się do stosunków podwykonawczych, wymagających zgody, o ile dotyczy to takich systemów IT, które są wymagane w celu świadczenia usług dla Zleceniodawcy. Prawa kontroli Zleceniodawcy  1. Zleceniodawca ma prawo na własny koszt przeprowadzać kontrole zlecenia za porozumieniem ze Zleceniobiorcą w normalnych godzinach pracy, nie utrudniając przebiegu pracy lub w indywidualnych przypadkach zlecić ich wykonanie audytorowi, o ile nie jest on w stosunku konkurencyjnym dla Zleceniobiorcy lub po stronie Zleceniobiorcy nie zachodzi inny, uzasadniony powód przeciwny takiej kontroli. Zleceniobiorca zobowiązuje się na polecenie Zleceniodawcy przekazać mu wymagane informacje, które są potrzebne do zapewnienia jego obowiązku kontroli zlecenia, oraz udostępniać wymagane dowody. 2. W odniesieniu do obowiązków kontrolnych Zleceniodawcy zgodnie z art. 28 ust. 1 RODO przed rozpoczęciem przetwarzania danych oraz w czasie zlecenia Zleceniobiorca gwarantuje, że Zleceniodawca może się przekonać co do stosowania się do podjętych środków techniczno-organizacyjnych. W tym celu Zleceniobiorca potwierdza na zapytanie Zleceniodawcy wdrożenie środków techniczno-organizacyjnych zgodnie z art. 32 RODO. Przy tym dowodem wdrożenia takich środków, które nie dotyczą konkretnego zlecenia, również poprzez przedłożenie aktualnej opinii, mogą być sprawozdania lub fragmenty sprawozdań (np. audytora, działu rewizji, inspektora danych osobowych, działu bezpieczeństwa IT, audytorów ochrony danych, audytorów jakości) lub odpowiednia certyfikacja audytu w zakresie bezpieczeństwa IT i ochrony danych (np. zgodnie z ochroną podstawową BSI) lub stosowanie się do zatwierdzonych zasad postępowania (tzw. BCR). Zleceniobiorca zastrzega sobie prawo do obciążenia Zleceniodawcy związanymi z tym kosztami na oddzielnej fakturze. 3. Jeżeli Zleceniodawca stwierdzi błędy lub nieprawidłowości w zakresie postanowień dotyczących ochrony danych, niezwłocznie poinformuje o tym fakcie Zleceniobiorcę.  Zgłoszenie w przypadku naruszenia przez Zleceniobiorcę  1. We wszystkich przypadkach Zleceniobiorca zdaje Zleceniodawcy raport, jeżeli na skutek jego działania lub działania zatrudnionych przez niego osób doszło do naruszenia przepisów w zakresie ochrony danych osobowych Zleceniodawcy lub postanowień zlecenia. 2. Wiadomym jest, że zgodnie z art. 33 RODO mogą zachodzić obowiązki informacyjne względem osób trzecich w przypadku zaginięcia lub nieprawidłowego przekazania lub uzyskania danych osobowych. W związku z tym należy niezwłocznie przekazywać takie przypadki Zleceniodawcy bez względu na winę. Obowiązuje to również w przypadku poważnych awarii pracy zakładu, podejrzenia innego naruszenia przepisów w zakresie ochrony danych osobowych lub innych nieprawidłowości w postępowaniu z danymi osobowymi Zleceniodawcy. Zleceniobiorca w kontakcie ze Zleceniodawcą podejmie odpowiednie środki w celu zabezpieczenia danych oraz zminimalizowania możliwych konsekwencji dla osób, których dane dotyczą. Jeżeli Zleceniodawca jest zobowiązany zgodnie z art. 33, 34 RODO, Zleceniobiorca będzie go wspierać w tym zakresie.  Upoważnienie do wydawania poleceń Zleceniodawcy  1. Z danych korzysta się wyłącznie w ramach podjętych postanowień i na polecenie Zleceniodawcy (zob. art. 28 ust. 3 str. 2 lit. a) RODO UE). Zleceniodawca zastrzega sobie prawo w ramach opisu zlecenia zgodnie z postanowieniem do szczegółowego wydawania poleceń odnośnie do rodzaju, zakresu i sposobu przetwarzania danych, które precyzuje na podstawie pojedynczych poleceń. Zmiany przedmiotu i sposobu przetwarzania są wspólnie ustalane i dokumentowane pisemnie. Informacje dla osób trzecich lub osób, których dane dotyczą, Zleceniobiorca przekazuje wyłącznie za uprzednią zgodą pisemną Zleceniodawcy. 2. Zleceniodawca niezwłocznie potwierdza polecenia ustne pisemnie lub drogą mailową (w formie tekstowej). Zleceniobiorca korzysta z danych wyłącznie w określonych celach i nie jest uprawniony do przekazywania ich osobom trzecim. Nie sporządza się kopii ani duplikatów danych bez wiedzy Zleceniodawcy. Nie dotyczy to kopii bezpieczeństwa, o ile są one konieczne do zapewnienia prawidłowego przetwarzania danych oraz danych, które są wymagane w celu stosowania się do ustawowych obowiązków przechowywania. 3. Zleceniodawca wyznacza osoby upoważnione do wydawania poleceń. Jeżeli Zleceniobiorca przetwarza dla Zleceniodawcy dane wrażliwe, Zleceniodawca bezpośrednio wyznaczy osoby upoważnione do wydawania poleceń, które podczas korzystania ze swoich uprawnień legitymują się nimi. Osoby upoważnione przez Zleceniodawcę do wydawania poleceń podane są w **Załączniku 1**. W przypadku, jeżeli u Zleceniodawcy i Zleceniobiorcy wyznaczona jest inna osoba upoważniona do wydawania poleceń, należy poinformować o tym pisemnie i zapisać w **Załączniku 1**. 4. Zleceniobiorca niezwłocznie poinformuje Zleceniodawcę zgodnie z art. 28 ust. 3 str. 3 RODO, jeżeli będzie zdania, że polecenie narusza przepisy w zakresie ochrony danych. Zleceniobiorca ma prawo wstrzymać wykonanie odpowiedniego polecenia tak długo, aż zostanie potwierdzone lub zmienione przez osobę odpowiedzialną po stronie Zleceniodawcy.  Usuwanie danych i zwracanie nośników danych po zakończeniu czynności  1. Po zakończeniu przetwarzania, a najpóźniej po zakończeniu umowy, Zleceniobiorca zwróci Zleceniodawcy wszystkie posiadane dokumenty i sporządzone rezultaty przetwarzania lub użytkowania lub dane utworzone w celu wykonania usługi lub skopiowane dane osobowe lub inne dane poufne, które są związane ze stosunkiem zlecenia lub za porozumieniem ze Zleceniodawcą zniszczy lub usunie je zgodnie z prawem ochrony danych. Materiał badany lub wybrakowany należy niezwłocznie zniszczyć zgodnie z prawem ochrony danych lub przekazać Zleceniodawcy. Zobowiązanie to dotyczy w takim samym stopniu ewentualnie zatrudnionych podwykonawców. Nie narusza to danych oraz kopii, które są wymagane w celu wykonania roszczeń z tytułu odpowiedzialności cywilnej lub rękojmi. 2. Dokumenty, które służą jako dowód prawidłowego przetwarzania danych zgodnie ze zleceniem lub ze względów prawnych, np. z powodu obowiązujących okresów przechowywania, nie mogą zostać zniszczone, przechowywane są przez Zleceniobiorcę zgodnie z obowiązującymi terminami po zakończeniu umowy, a po upływie terminu przechowywania zostaną niezwłocznie zniszczone. Należy poinformować Zleceniodawcę o rodzaju i zakresie danych przechowywanych zgodnie z ust. 1 lub 2. Zleceniobiorca może przenieść te dane po zakończeniu umowy na Zleceniodawcę w celu zwolnienia z obowiązku. 3. Zleceniobiorca po zakończeniu umowy potwierdzi Zleceniodawcy bezpieczne usunięcie lub zniszczenie posiadanych przez niego dokumentów.  Okres obowiązywania umowy i rozwiązanie  1. Niniejsza umowa wchodzi w życie w momencie jej podpisania i zostaje zawarta na czas nieokreślony, w każdym razie na tak długo, jak umowa główna. Prawo do wypowiedzenia zwyczajnego jest zgodne z umową główną 2. W uzupełnieniu do umowy głównej ustala się, że naruszenie postanowień ustawowych i umownych w zakresie ochrony danych przez Zleceniobiorcę zawsze jest istotnym powodem dla Zleceniodawcy, aby skorzystać z prawa do rozwiązania umowy w trybie nadzwyczajnym. W związku z tym Zleceniodawca może rozwiązać umowę główną z ważnych powodów bez zachowania terminu. 3. Jeżeli znacząco zmienią się podstawy wykonania umowy lub w pełni nie będą obowiązywać z powodu zmiany stanu prawnego lub ustawowego lub naruszenia lub innych środków organów nadzorczych, obydwie strony mają prawo do dostosowania niniejszej umowy do nowych warunków, o ile jest to możliwe lub dopuszczalne przez obydwie strony. Jeżeli nie ma możliwości dostosowania umowy lub jest to niedopuszczalne dla jednej ze stron, jest to ważny powód dla obydwu stron do rozwiązania umowy bez zachowania terminu wypowiedzenia. Nie narusza to ust. 2.  Postanowienia końcowe  1. Jeżeli jedno postanowienie niniejszej umowy jest albo okaże się nieważne, nie narusza to obowiązywania umowy. W takim przypadku strony ustalają inne postanowienie, które odpowiada treści i celowi ekonomicznemu postanowienia nieważnego. 2. Zmiany i uzupełnienia do niniejszej umowy, poszczególnych umów indywidualnych i ich części składowych wymagają formy pisemnej pod rygorem nieważności. Zasada ta dotyczy również rezygnacji z klauzuli o konieczności zastosowania formy pisemnej. 3. Zarzut prawa zatrzymania w rozumieniu § 273 niemieckiego kodeksu cywilnego w odniesieniu do przetwarzanych danych i właściwych nośników danych zostaje wyłączony. 4. Stosunki prawne partnerów podlegają prawu Republiki Federalnej Niemiec z wyłączeniem Konwencji Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów oraz z wyłączeniem poszczególnych regulacji prawa niemieckiego, które wskazują na inny porządek prawny niż niemiecki. 5. Wszystkie spory związane z niniejszą umową podlegają sądowi właściwemu określonemu w umowie głównej, o ile jest to dopuszczalne. 6. Jeżeli regulacje poszczególnych przepisów niniejszej umowy wykraczają poza czas jej obowiązywania, przepisy te pozostają w mocy do momentu ustania obowiązywania umowy. 7. Załączone do niniejszej umowy załączniki stanowią jej istotną część składową.   **Załącznik 1: Porozumienia w sprawie przetwarzania danych**  **Załącznik 2: Porozumienia w sprawie określenia środków technicznych i organizacyjnych**   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |  | Miejscowość, data |  | Miejscowość, data | |  |  |  |  | |  | Zleceniodawca  Nazwisko / podpis / pieczęć firmowa |  | Zleceniobiorca  Mathias Heese / Prezes  Martin Behrend / VP Finance  Nazwisko / podpis / pieczęć firmowa | |