Policy/Richtlinie

Title/Titel:	Privacy and Integrity Policy/Richtlinie zu Datenschutz und Integrität
Number/Nummer:	POL COR-007
Version/Version:	12
Department/Abteilung:	Corporate/Konzern
Effective Date/Gültigkeitsdatum:	04OCT2019

Approvals/Freigaben

The titles indicated below are reflective of the area responsible at the time of approval. Electronic signatures for all approvers are maintained on file.

Die unten angegebenen Titel spiegeln den Bereich der Verantwortlichkeit zum Zeitpunkt der Freigabe wieder. Elektronische Signaturen für alle Freigaben werden in den Unterlagen geführt.

Date Issued for Approval/ Geplantes Freigabedatum:	23AUG2019
Author/Autor:	Veronica Contreras
Title/Department/Titel/Abteilung:	Data Privacy Officer, Counsel/Quality Management
Management/Management:	Achim Schuelke
Title/Department/Titel/Abteilung:	Executive Vice President, Product Line Executive
Management/Management:	Juergen Kasprowitsch
Title/Department/Titel/Abteilung:	Senior Director, Quality Assurance/Regulatory Affairs/Quality Management
Management/Management:	Michele Buonopane
Title/Department/Titel/Abteilung:	Vice President, Human Resources/Human Resources
Quality Management/ Qualitätsmanagement:	Richard Miller
Title/Department/Titel/Abteilung:	Vice President, Quality Management/Quality Management

1. Overview/Übersicht

The purpose of this Privacy and Integrity Policy ("Policy") is to define and outline the company's data privacy and security governance program ("Program") requirements that support Program requirements and this Policy. Such practices enable eResearchTechnology, Inc. (and each of its subsidiaries and affiliates, including Biomedical Systems B.V.B.A, eResearchTechnology GmbH, PHT Corporation SARL, eResearch Technology Limited, ERT, Inc. KK, and U.S. Biomedical Systems India Pvt. Ltd., collectively "ERT") to appropriately manage its privacy and security risks.

Der Zweck dieser Richtlinie zu Datenschutz- und Integrität („Richtlinie") ist es, die Anforderungen des Datenschutz- und Sicherheitsrichtlinienprogramms („Programm") des Unternehmens zu definieren und zu skizzieren, die die Anforderungen des Programms und dieser Richtlinie unterstützen. Solche Praktiken ermöglichen es eResearchTechnology, Inc., (und jede ihrer Tochtergesellschaften und verbundenen Unternehmen, eResearchTechnology GmbH, PHT Corporation SARL, eResearch Technology Limited, ERT, Inc. KK, and U.S. Biomedical Systems India Pvt. Ltd. gemeinsam „ERT"), ihre Datenschutz- und Sicherheits-risiken angemessen zu managen.

ERT is committed to this Policy in protecting the privacy, integrity, and security of those who entrust us with their personal, clinical, protected health information, or individually identifiable health information ("Data," as further defined below) that ERT may access, collect, acquire, use, disclose, store, transfer, retain, or dispose of in all aspects of its business worldwide.

ERT verpflichtet sich zu dieser Richtlinie, um die Privatsphäre, Integrität und Sicherheit derjenigen zu schützen, die uns ihre persönlichen, klinischen, geschützten Gesundheitsinformationen oder individuell identifizierbaren Gesundheitsinformationen („Daten", wie unten näher beschrieben) anvertrauen, auf die ERT in allen Aspekten seiner Geschäftstätigkeit weltweit zugreift, sammelt, erwirbt, verwendet, offenlegt, speichert, überträgt, aufbewahrt oder über die ERT verfügen kann.

This Policy provides ERT management guidance for maintaining compliance with company data privacy and security standards, including the ERT General Data Protection Regulation ("GDPR") Policy, the ERT Health Insurance Portability and Accountability Act Policy, applicable laws and regulations, such as the General Data Protection Regulation ("GDPR"), the Act on Protection of Personal Information ("APPI"), the Health Insurance Portability and Accountability Act of 1996

Diese Richtlinie enthält ERT-Management-Leitlinien für die Einhaltung der unternehmensinternen Datenschutz- und Sicherheitsstandards, einschließlich der ERT-Richtlinie zur allgemeinen Datenschutzverordnung (DSGVO), der ERT-Richtlinie zur Übertragbarkeit und Rechenschaftspflicht im Bereich der Krankenversicherung, der geltenden Gesetze und Vorschriften, wie z.B. der Allgemeinen Datenschutzverordnung (DSGVO), dem Act on Protection of Personal

("HIPAA"), ICH E6 GCP, world regulatory authorities, the Helsinki accords, applicable to research with human subjects, and the EU-US and Swiss-US Privacy Shield Frameworks.

Information (APPI), des Health Insurance Portability and Accountability Act von 1996 (HIPAA), der ICH E6 GCP, der Weltaufsichtsbehörden, der Helsinki-Abkommen, die für die Forschung mit Menschen gelten, sowie der EU-US und Swiss-US Privacy Shield Frameworks.

The following regulations are applicable to this policy:

- UK Medicines and Healthcare Products Regulatory Agency ("MHRA")
- US Food and Drug Administration ("FDA")
- European Medicines Agency (EMA)
- US Department of Health and Human Services ("DHHS")
- UK Information Commissioner's Office ("ICO")
- International Conference on Harmonisation - Good Clinical Practice ("ICH-GCP")
- International Organization for Standardization (ISO)
- China Food and Drug Administration ("CFDA")
- Pharmaceuticals and Medical Devices Agency ("PMDA")

Die folgenden Bestimmungen gelten für diese Richtlinie:

- Die britische Regulierungsbehörde für Arzneimittel und Gesundheitsprodukte („MHRA");
- Die US Food and Drug Administration („FDA");
- Die Europäische Arzneimittel-Agentur („EMA");
- Das United States Department of Health and Human Services ("DDHS")
- Das Information Commissioner's Office („ICO");
- Die International Conference on Harmonization - Good Clinical Practice („ICH-GCP R2");
- Die Internationale Organisation für Normung („ISO");
- Die China Food and Drug Administration („CFDA"); und
- Die Arzneimittel- und Medizinproduktebehörde („PMDA")

This Policy applies to all Personnel (as defined below) and any other Agent (as defined below) who may, during their business relationship with ERT, access, collect, acquire, use, disclose, store, transfer, retain, or dispose of Data (collectively "Use," "Used," or "Using").

Diese Richtlinie gilt für alle Mitarbeiter (wie unten definiert) und alle anderen Vertreter (wie unten definiert), die während ihrer Geschäftsbeziehung mit ERT auf Daten zugreifen, diese sammeln, erwerben, verwenden, offenlegen, speichern, übertragen, aufbewahren oder veräußern können („verwenden", „verwendeten"oder "in Verwendung").

2. Related Documents/Mitgeltende Unterlagen

Document Number/ Dokumentennummer	Document Name/Dokumentenname
POL COR-004	Record Retention Policy
POL COR-005	Security Policy
POL COR-009	ERT HIPAA Privacy Policy
POL COR-011	Acceptable Use Policy
POL COR-014	General Data Protection Regulation (GDPR) Policy
SOP 119	Product Life Cycle
SOP 122	Unauthorized Disclosure/Data Breach Management
SOP 123	Subject Access Request
SOP 1300	Development Life Cycle
FORM 007_01	Employment Informed Consent Form
N/A	21 CFR Part 11: Electronic Records; Electronic Signatures, August 1997 (FDA website)
N/A	EU General Data Protection Regulation (GDPR) 2016/679 (www.ico.org.uk)
N/A	Directive 2000/31/EC on electronic commerce (http://ec.europa.eu/internal_market/e-commerce/directive/index_ en.htm)
N/A	EU GCP Directive 2005/28/EC, April 2005 (EurLex website)
N/A	Guidance for Industry - 21 CFR Part 11; Electronic Records; Electronic Signatures - SCOPE AND APPLICATION (August 2003) (FDA website)
N/A	Guidance for Industry: Computerized Systems Used In Clinical Investigations, May 2007 (FDA website)
N/A	Guidance for Industry: E6 Good Clinical Practice, April 1996 (ICH website)
N/A	ERT Privacy Shield Certification (US Department of Commerce website)
N/A	HIPAA Security and Privacy Rule, 45 CFR Part 164 [Electronic Code of Federal Regulations (e-CFR) website]
N/A	EU-US and Swiss-US Privacy Shield Frameworks: A Guide to Self-Certification. Including the full text of the official declaration of the Privacy Shield Privacy Principles as announced on July 12, 2016 (US Dept. of Commerce website. http://www.export.gov).

Document Number/ Dokumentennummer	Document Name/Dokumentenname
N/A	US Better Business Bureau (http://www.bbb.org/EUprivacy-shield/)

3. Definitions/Definitionen

Term/Begriff	Definition/Definitionen	
Agent/ Vertreter	A third-party, including consultants, that may access, collect, acquire, use, disclose, store, transfer, retain, or dispose of Data (and Sensitive Personal Data, where applicable) on behalf of, and under the instructions of ERT, in order to carry out ERT business activities or operations on the company's behalf.	Dritte, einschließlich Berater, die im Namen und auf Anweisung von ERT auf Daten (und gegebenen-falls auf sensible personenbezo-gene Daten) zugreifen, diese sammeln, erwerben, verwen-den, offenlegen, speichern, übertragen, aufbewahren oder über diese verfügen können, um im Namen von ERT geschäftliche Aktivitäten oder Operationen durchzuführen.
Data/ Daten	Any personal, clinical, protected health information, individually identifiable health information, relating to an identified or identifiable natural person (i.e., a Data Subject). A "Data Subject" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, telephone number, email address, address information, social security number, date of birth, IP address, an identification number, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a data subject.	Alle personenbezogenen, klini-schen, geschützten Gesundheitsin-formationen, individuell identifizier-baren Gesundheitsinformationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, d.h. eine betroffene Person, be-ziehen. Eine „betroffene Person" ist eine Person, die direkt oder indirekt identifiziert werden kann, insbeson-dere durch Bezugnahme auf einen Identifikator, wie beispielsweise: Name, Telefonnummer, E-Mail-Adresse, Adressinformationen, Sozialversicherungsnummer, Geburtsdatum, IP-Adresse, eine Identifikationsnummer oder auf einen oder mehrere Faktoren, die spezifisch für die physische, physiologische, genetische, men-tale, wirtschaftliche, kulturelle oder

	Data may also include "Sensitive Personal Data" that reveals a data subject's race, ethnic origin, political opinions, criminal convictions and offences, biometric information, genetics, religious or philosophical beliefs, or trade union membership, or that concerns an individual's health or sex life. Data will be treated as Sensitive Personal Data where it is received from an Agent that treats and identifies it as sensitive. Data does not include information, so long as it is anonymized or de-identified.	soziale Identität einer betroffenen Person sind. Zu den Daten können auch „sensible personenbezogene Daten" gehören, die die Rasse, die ethnische Herkunft, politische Meinungen, strafrechtliche Verurteilungen und Handlungen, biometrische Daten, genetische, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit einer Person offenbaren oder die die Gesundheit oder das Sexualleben einer Person betreffen. Darüber hinaus werden Informationen als sensible personenbezogene Daten behandelt, wenn sie von einem Dritten erhalten werden, der sie als vertraulich behandelt und identifiziert. Daten beinhalten keine Informationen, sofern sie anonymisiert oder de-identifiziert sind.
Data Breach/ Datenschutzverletzung	The acquisition, access, use, or disclosure of unsecured Data in a manner not permitted under applicable data privacy and security laws and regulations, including GDPR, APPI, and HIPAA, which poses a significant financial, reputational, or other harm to the affected individual.	Definiert als Erwerb, Zugriff, Nutzung oder Offenlegung ungesicherter Daten in einer Weise, die nach den geltenden Datenschutz- und Datensicherheitsgesetzen und -vorschriften, einschließlich DSG VO, APPI und HIPAA, nicht zulässig ist und der betroffenen Person einen erheblichen finanzi-ellen, reputationellen oder sonsti-gen Schaden zufügen könnte.
Data Integrity/ Datenintegrität	Accuracy and consistency pertaining to the systems and processes for Data capture, correction, maintenance, transmission, and retention.	Genauigkeit und Konsistenz in Bezug auf die Systeme und Prozesse zur Datenerfassung, -korrektur, -wartung, -übertragung und -speicherung.

Data Quality/ Datenqualität	Condition of the Data (i.e., the quality is acceptable for the intended use).	Zustand der Daten, d.h. die Qualität ist für den vorgesehenen Einsatz-zweck akzeptabel.
Data Security/ Datensicherheit	Degree to which Data are protected from the risk of accidental or malicious alteration or destruction and from unauthorized access, use, or disclosure in accordance with the Data Risk Classification Chart included within this document and ERT's POL COR-005 Security Policy.	Der Grad, zu dem die Daten vor dem Risiko einer versehentlichen oder böswilligen Änderung oder Zerstörung und vor unbefugtem Zugriff, Verwendung oder Offen-legung geschützt sind, gemäß der Tabelle zur Klassifizierung des Datenrisikos („Tabelle"), die dieser als Anlage 1 beigefügt ist, und der ERT Sicherheitsrichtlinie POL COR-005.
eCommerce/ eCommerce	Use of electronic systems and networks by consumers, sellers, and other entities to conduct business activities.	Nutzung elektronischer Systeme und Netzwerke durch Verbraucher, Verkäufer und andere Stellen zur Durchführung von Geschäftsakti-vitäten.
ERT Systems and Processes/ ERT Systeme und Prozesse	Devices and applications that capture trial Data, transmission technologies, software applications for storage and review of Data, registrations for users, processes for identification, qualification and training of users, including actions on electronic (and related paper records) that rely on security and authenticity protections provided by ERT for conducting clinical investigations, diagnostic evaluations, and other services delivered to clients.	Geräte und Anwendungen zur Erfassung von Versuchsdaten, Übertragungstechnologien, Soft-wareanwendungen zur Speiche-rung und Überprüfung von Informa-tionen, Registrierungen für Be-nutzer, Verfahren zur Identifizie-rung, Qualifizierung und Schulung von Benutzern, generell einschließ-lich aller Maßnahmen in Bezug auf elektronische (und zugehörige Papierunterlagen), die auf Sicherheits- und Authentizitäts-schutz durch ERT zur Durchführung klinischer Untersuch-ungen, diagnostischer Bewert-ungen und anderer an Kunden erbrachter Dienstleistungen beru-hen.

Patient/ Patient	Person under a physician's care for a particular disease or condition. **Note:** A Subject in a clinical trial is not necessarily a Patient, but a Patient in a clinical trial is a Subject. See also Subject. Although, often used interchangeably as a synonym for Subject, a healthy volunteer is not a Patient.	Person, die von einem Arzt auf Grund einer bestimmten Krankheit oder eines bestimmten Zustands betreut wird. **Hinweis:** Ein Teilnehmer einer klinischen Studie ist nicht unbedingt ein Patient, aber ein Patient in einer klinischen Studie ist immer ein Teilnehmer. Siehe auch betroffene Person. Auch wenn der Begriff oft als austauschbares Synonym für betroffene Person verwendet wird, ist ein gesunder Freiwilliger kein Patient.
Personnel/ Personal	ERT current, past, and prospective employees, trainees, temporary workers, contractors, or applicants.	Bedeutet aktuelle, ehemalige und zukünftige ERT-Mitarbeiter, Auszubildende, Zeitarbeiter, Auftragnehmer oder Bewerber.
Privacy Protection/ Schutz der Privatsphäre	The appropriate use of Data or Sensitive Personal Data under specific circumstances. What is appropriate will depend on context, law, and the individual's expectations.	Die angemessene Verwendung von Daten oder sensiblen personenbezogenen Daten unter bestimmten Umständen. Was angemessen ist, hängt vom Kontext, dem Gesetz und den Erwartungen des Einzelnen ab.
Security Incident/ Sicherheitsrelevantes Ereignis	An attempted or successful unauthorized access, use, disclosure, modification, or destruction of Data or interference with system operations in an information system.	Ein versuchter oder erfolgreicher unbefugter Zugriff, die Nutzung, Offenlegung, Änderung oder Zerstörung von Daten oder Beeinträchtigung des Systembetriebs in einem Informationssystem.
Sponsor/ Sponsor	An individual, company, institution, or organization which takes responsibility for the initiation, management, or financing of a clinical trial.	Eine Person, ein Unternehmen, eine Institution oder eine Organi-sation, welche(s) die Verantwor-tung für die Einleitung, das Management oder die Finanzierung einer klinischen Studie übernimmt.

Subject/ Betroffene Person	An individual who participates in a clinical trial, either as recipient of the investigational product(s), or as a control.	Eine Person, die an einer klinischen Studie teilnimmt, entweder als Empfänger des/der Prüfpräparate(s) oder als Kontrolle, sowie involviertes ERT Personal.
Unauthorized Disclosure/ Unbefugte Offenlegung	An incident involving Data exposure to a Data Subject(s), or entity(ies), not authorized to access such Data.	Ein Vorfall, der die Datensicherheit gegenüber einer oder mehreren Personen oder Einheit(en) betrifft, die nicht berechtigt sind, auf diese Daten zuzugreifen.

4. Roles and Responsibilities/Rollen und Verantwortlichkeiten

The following roles and responsibilities are required by this Policy:

Die folgende Tabelle enthält die für diese Politik erforderlichen Stellen und Verantwortungsbereiche:

Role/Rolle	Responsibilities/Verantwortlichkeiten	
Data Protection/Privacy Officer(s) ("DPO(s)")/Director of Security and Risk Management ("Security Director")/ **Datenschutzbeauftragte(r) – („DPO(s)")/ „Sicherheitsdirektor"**	The DPO(s) and Security Director are responsible for the development, implementation, enforcement, and monitoring of Program requirements to ensure that ERT complies with applicable US, EU, and regional privacy and security laws and regulations and conforms to industry best practices for clinical trial, healthcare, and privacy.	Der/die DPO und der Sicherheitsbeauftragte sind für die Entwicklung, Umsetzung, Durchsetzung und Überwachung der Programmanforderungen verantwortlich, um sicherzustellen, dass ERT die geltenden Datenschutzgesetze und -vorschriften der USA, der EWU und der Schweiz einhält und mit den branchenweit besten Praktiken für klinische Studien, Gesundheitsversorgung und Datenschutz übereinstimmt.
Quality Management/ Qualitätsmanagement	Department that is responsible for auditing Program requirements, in conjunction with other key stakeholders, where required.	Abteilung, die für die Auditierung der Programmanforderungen verantwortlich ist, bei Bedarf in Zusammenarbeit mit anderen wichtigen Interessengruppen.

5. Policy/Richtlinie

5.1 Program Requirements/Programmanforderungen

ERT shall implement a Program that identifies key compliance elements and corresponding compliance documentation.

ERT realisiert ein Programm, in dem die wichtigsten Konformitätselemente und die entsprechenden Konformitätsdokumente fest-gelegt sind.

This Policy and applicable Program documentation shall ensure compliance with ERT's Code of Ethics standards and Program hierarchy, as further identified, without limitation in the chart below.

Diese Richtlinie und die dazugehörige Programmdokumentation müssen die Einhal-tung der ERT-Ethikstandards und der Programmhierarchie ohne Einschränkung gewährleisten, wie sie in der folgenden Tabelle näher erläutert werden.

Privacy	**Program Infrastructure**	**Security**
Code of Ethics Ethikkodex		**Code of Ethics** Ethikkodex
Privacy and Integrity Policy Richtlinie zu Datenschutz und Integrität **GDPR Policy** DSGVO Richtlinie **HIPAA Privacy Policy** HIPAA-Datenschutzrichtlinie	**Code of Ethics/ *Ethikkodex*** **Policies/ *Richtlinien*** **Procedures/ *Verfahren*** **Templates and Forms/*Vorlagen und Formulare***	**Security Policy** Sicherheitsrichtlinien **Acceptable Use Policy** Akzeptable Nutzungsrichtlinien **BYOD and End-User Management** BYOD und Endbenutzermanagemen
Unauthorized Disclosure/Data Breach Management Handhabung von unbefugten Offenlegungen/Datenschutzverletzungen **Subject Access Request** Zugangsanfrage durch den Betroffenen **Product Life Cycle** Produktlebenszyklus		**Incident Management** Ereignismanagement **Product Life Cycle** **Produktlebenszyklus** **Access Management** Zugriffsmanagement **Security Management** Sicherheitsmanagement
Data Privacy Impact Assessment Abschätzung der Auswirkungen auf die Privatsphäre **Data Processing Agreements** Datenverarbeitungsvereinbarungen **Employment Informed Consent Form** Formular zur Zustimmung nach Inkenntnissetzung bei Einstellung		**Security Impact Assessment** Bewertung der Sicherheitsauswirkungen **Incident Response Plan** Ereignisreaktionsplan

Program supporting policies and procedures shall comprise of, without limitation, this Policy, ERT's General Data Protection Regulation Policy ("GDPR"), the ERT Health Insurance Portability and Accountability Act

Programmunterstützende Richtlinien und Verfahren umfassen uneingeschränkt diese Richtlinie, die ERT Datenschutzgrund-verordnung („DSGVO"), die ERT-Richtlinie „Health Insurance Portability and

("HIPAA") Policy, ERT's Security Policy, ERT's Acceptable Use Policy, and related ERT Standard Operating Procedures, such as Unauthorized Disclosure/Data Breach Management, Subject Access Request, and Product Life Cycle.

Accountability Act" („HIPAA"), die ERT Sicherheitspolitik, die ERT Acceptable Use Policy und die damit verbundenen ERT-Standardarbeitsverfahren, wie z.B.: die Handhabung von unbefugten Offenlegungen/Datenschutzverletzungen, Anträge auf Zugang durch den Betroffenen und den Produktlebenszyklus.

Additional supporting Program documentation shall include, without limitation, a data privacy compliance matrix; master service agreement templates, data processing agreement templates and corresponding security exhibit, employment informed consents, a, unauthorized disclosure reporting form and corresponding tracker, training materials, a Privacy and Security Governance Overview, and any other applicable supporting documentation necessary for overall Program compliance.

Zusätzliche Begleitdokumentationen des Programms umfassen unter anderem: eine Matrix zur Einhaltung des Datenschutzes, Vorlagen für Rahmen-Servicevereinbarungen, Vorlagen für Datenverarbeitungsverträge und entsprechende Sicherheitsanlagen, Einwilligungen in Bezug auf die Beschäftigung, ein Formular zur Meldung von unbefugten Offenlegungen und den entsprechenden Tracker, Schulungsmaterialien, einen Überblick über die Governance für Datenschutz und Sicherheit und alle anderen anwendbaren Begleitdokumente, die für die Einhaltung des gesamten Programms erforderlich sind.

All applicable Program documentation shall align with the Policy principles herein and shall meet ERT's risk-based data privacy categorizations as further documented in the Data Risk Classification Chart.

Alle anwendbaren Programmdokumentationen müssen mit den hierin enthaltenen Richtlinien-prinzipien übereinstimmen und den risiko-basierten Datenschutzkategorien von ERT entsprechen, wie sie in der Grafik näher beschrieben sind.

5.2 Data Privacy Risk Categorization/Kategorisierung des Datenschutzrisikos

ERT shall establish a data privacy risk categorization that establishes data types and associated risk rankings, as further outlined in the Data Risk Classification Chart.

ERT erstellt eine Risikokategorisierung für den Datenschutz, die die Datentypen und die damit verbundenen Risikoeinstufungen festlegt, wie in der Grafik näher erläutert.

ERT shall establish a data privacy risk categorization that establishes data types and associated risk rankings, as further outlined in the Data Risk Classification Chart.

Die Datensicherheitskontrollen werden in Übereinstimmung mit der Risikoeinstufung der Tabelle und den Anforderungen der geltenden Datenschutzgesetze und -vorschriften vergeben.

5.3 General Data Privacy Principles/Allgemeine Datenschutzgrundsätze

ERT complies with the EU-US and Swiss-US Privacy Shield Frameworks, as set forth by the US Department of Commerce regarding Data collection, use, and retention from European Union member countries and Switzerland. ERT shall ensure compliance with the standards, as documented within this Policy.

ERT hält sich an die EU-US und Swiss-US Privacy Shield Frameworks des US-Handelsministeriums bezüglich der Datenerfassung, -verwendung und -speicherung durch Mitgliedsländer der Europäischen Union und der Schweiz. ERT stellt sicher, dass die Normen, wie in dieser Richtlinie beschrieben, eingehalten werden.

ERT shall ensure, to the best of its ability that Data is correct, accessible, and conforms to 21 CFR Part 11/Annex 11 controls.

ERT stellt nach bestem Wissen und Gewissen sicher, dass die Daten korrekt und zugänglich sind und den 21 CFR Teil 11/Annex 11 Kontrollen entsprechen.

ERT shall ensure that site investigators can fulfill their regulatory obligations to maintain and retain records obtained using ERT Systems and Processes about Subjects in a clinical investigation.

ERT stellt sicher, dass die Prüfer vor Ort ihren gesetzlichen Verpflichtungen zur Aufrechterhaltung und Aufbewahrung der mit ERT-Systemen und -Prozessen über die Probanden in einer klinischen Prüfung erhaltenen Aufzeichnungen nachkommen können.

ERT shall ensure that sites have the applicable tools available and documentation in order to provide Subjects access to Data during and after a clinical investigation.

ERT stellt sicher, dass den Standorten die entsprechenden Tools und Dokumentationen zur Verfügung stehen, um den betroffenen Personen während und nach einer klinischen Prüfung Zugang zu den Daten zu gewähren.

ERT shall disclose to Sponsors and site investigators (who must comply with regulations pertaining to clinical research and eCommerce) applicable Data required to fulfill regulatory responsibilities under FDA 21CFR 312 subpart D for Data Integrity, in clinical trials, for medical products, using ERT Systems and Processes. Data Integrity shall be clear-cut, validated, and auditable.

ERT wird Sponsoren und Prüfern (welche die Vorschriften für klinische Forschung und eCommerce einhalten müssen) die anwendbaren Daten offenlegen, die zur Erfüllung der regulatorischen Aufgaben gemäß FDA 21CFR 312 Unterabschnitt D für Datenintegrität in klinischen Studien, für Medizinprodukte unter Verwendung von ERT-Systemen und -Prozessen erforderlich sind. Die Datenintegrität muss klar definiert, validiert und prüfbar sein.

ERT shall ensure that any Data Use by its Personnel or Agents (where applicable) are done only to perform the applicable service, only the minimum amount of Data is Used, and

ERT stellt sicher, dass die Datennutzung durch ihr Personal oder ihre Vertreter (falls zutreffend) nur zur Erbringung der entsprechenden Dienstleistungen erfolgt,

such Use is done in accordance with Program requirements, this Policy, and applicable data privacy and security laws and regulations.

dass nur die minimale Datenmenge verwendet wird und dass diese Nutzung in Übereinstimmung mit den Programmanforderungen, dieser Richtlinie und den geltenden Gesetzen und Vorschriften zum Datenschutz und zur Datensicherheit erfolgt.

ERT shall comply with Data disclosure requests, it may be required to fulfill, under the investigatory and enforcement powers of the Federal Trade Commission and any other applicable regulatory agencies identified under this Policy.

ERT wird den Anforderungen an die Offenlegung von Daten nachkommen und kann verpflichtet sein, auch solche im Rahmen der Untersuchungs- und Durchsetzungsbefugnisse der Federal Trade Commission und aller sonstigen in dieser Richtlinie genannten zuständigen Regulierungsbehörden zu erfüllen.

Adherence by ERT to these General Data Privacy Principles and Access may be limited to the extent required to meet any other legal, governmental, national security, or public interest obligations.

Die Einhaltung dieser Allgemeinen Datenschutzgrundsätze und des Zugangs durch ERT kann, soweit erforderlich, eingeschränkt werden, um anderen rechtlichen, staatlichen, die nationale Sicherheit betreffenden Verpflichtungen oder Verpflichtungen im öffentlichen Interesse nachzukommen.

5.4 Personnel Data Collection and Access/Personaldaten - Erfassung und Zugriff

Data and Sensitive Personal Data related to Personnel are subject to Privacy Protection and Data Security, in accordance with this Policy, the Data Risk Classification Chart, and all applicable US, EU, Swiss, and regional privacy laws and regulations.

Daten und sensible personenbezogene Daten, die sich auf die betroffenen Personen beziehen, unterliegen dem Datenschutz und der Datensicherheit in Übereinstimmung mit dieser Richtlinie, der Tabelle und allen anwendbaren Datenschutzgesetzen und –vorschriften der USA, der EWR und der Schweiz.

ERT Uses Personnel Data or Sensitive Personal Data in a transparent way and only shares or discloses such Data for the following reasons, including without limitation (i) employee management and administration (including both during and after employment); (ii) employment verification; (iii) administering employee benefits; (iv) administering personal short or long-term compensation programs or

ERT verwendet Personaldaten oder sensible personenbezogene Daten auf transparente Weise und gibt diese nur aus den folgenden Gründen weiter oder legt diese offen, insbesondere: (i) Mitarbeitermanagement und -verwaltung (einschließlich während und nach dem Arbeitsverhältnis); (ii) Beschäftigungsverifizierung; (iii) Verwaltung von Sozialleistungen; (iv) Verwaltung von persönlichen

benefits; (v) evaluating performances; (vi) managing corporate programs;(vii) conducting disciplinary proceedings; (viii) addressing labor relations issues; (ix) processing health insurance claims; and (x) Data share with Agents for related employment services, including payroll processors and support services. Any request to share Data or Sensitive Personal Data with non-Agents shall only occur if authorized by the individual in writing, subject to other legal and regulatory requirements.

kurz- oder langfristigen Vergütungsprogrammen oder -leistungen; (v) Bewertung von Leistungen; (vi) Verwaltung von Unternehmensprogrammen; (vii) Durchführung von Disziplinarverfahren; (viii) Behandlung von Angelegenheiten im Bereich der Arbeitsbeziehungen; (ix) Bearbeitung von Krankenversicherungsansprüchen und (x) Datenaustausch mit Vertretern für verbundene Arbeitnehmerdienste, einschließlich Verarbeitern von Lohndaten und Unterstützungsdienste. Jede Anfrage zur Weitergabe von Daten oder sensiblen personenbezogenen Daten an Nicht-Vertreter darf nur erfolgen, wenn sie von der Person schriftlich genehmigt wurde, vorbehaltlich anderer gesetzlicher und regulatorischer Anforderungen.

ERT will manage Data and Sensitive Personal Data of its Personnel from both foreign and domestic office locations, to ERT corporate headquarters located in the United States of America, in accordance with the Data Risk Classification Chart classifications, Form-007_01 Employment Informed Consent Form, and Program requirements.

ERT wird Daten und sensible personenbezogene Daten seines Personals (sowohl von ausländischen als auch von inländischen Niederlassungen bis hin zur ERT-Unternehmenszentrale in den Vereinigten Staaten von Amerika) in Übereinstimmung mit den Klassifizierungen der Tabelle, Formular Form-007_01 Employment Informed Consent Form und den Anforderungen des Unternehmensprogramms, verwalten.

5.5 Sites, Subjects, Sponsors, and Agents Collection and Access/Standorte, betroffene Personen, Sponsoren und Vertreter - Erhebung und Zugriff

Data and Sensitive Personal Data collected from Patients or Subjects, sites, Sponsors, and Agents (during clinical research activities) are subject to Privacy Protection and Data Protection, in accordance with this Policy, the Data Risk Classification Chart, protections contractually agreed to, and applicable data privacy and security laws and regulations.

Daten und sensible personenbezogene Daten, die von Patienten oder betroffenen Personen, Standorten, Sponsoren und Vertretern (während der klinischen Forschungs-tätigkeiten) erfasst werden, unterliegen dem Schutz der Privatsphäre und dem Datenschutz, der Übereinstimmung mit dieser Richtlinie, der Tabelle, dem vertraglich verein-barten Schutz und den anwendbaren Ge-setzen und Vorschriften des Datenschutzes.

Patient information required to be disclosed to Sponsors shall be pseudonymized (i.e., individual identifying factors are given unique identifiers, which ERT holds no access to any re-identification key, so that only certain demographic information (e.g. an ID code) is visible) or anonymized or de-identified (i.e. no Personal Data, or Sensitive Personal Data, are available because all individual identifying factors have been completely removed). Sponsors shall not have access to Data or Sensitive Personal Data from Subjects beyond what is defined and allowed within the applicable study protocol and informed consent disclosures.

Patienteninformationen, die an Sponsoren weitergegeben werden müssen, müssen pseudonymisiert werden (d.h. einzelne Identifizierungsfaktoren erhalten eindeutige Identifikatoren, die ERT keinen Zugang zu einem Re-Identifikationsschlüssel gewähren, so dass nur bestimmte demografische Informationen (z.B. ein ID-Code) sichtbar sind) oder anonymisierte oder de-identifizierte (d.h. keine personenbezogenen Daten oder sensible personenbezogene Daten sind verfügbar, da alle einzelnen Identifizierungs-faktoren vollständig entfernt wurden). Sponsoren dürfen keinen Zugang zu Daten oder sensiblen personenbezogenen Daten von Probanden haben, die über das hinausgehen, was im Rahmen des anwendbaren Studienprotokolls und der Offenlegung der Einwilligungserklärung definiert und erlaubt ist.

Data requiring disclosure to site investigators, who have clinical responsibility for Patients in the trial, for purposes of reviewing clinically relevant Data or Sensitive Personal Data, are subject to Privacy Protection and Data Security, in accordance with this Policy, the Data Risk Classification Chart, Program requirements, and other applicable data privacy and security protections

Daten, die an Prüfer vor Ort weitergegeben werden müssen, die die klinische Verantwortung für Patienten in der Studie tragen, um klinisch relevante Daten oder sensible personenbezogene Daten zu überprüfen, unterliegen dem Datenschutz und der Datensicherheit in Übereinstimmung mit dieser Richtlinie, der Tabelle, den Programm-anforderungen und anderen anwendbaren Datenschutz- und Sicherheitsvorschriften.

ERT will not share Data, or Sensitive Personal Data, about Subjects, site-staff, or Sponsor personnel with Agents, unless those parties are contractually bound to adhere to substantially the same Program and quality procedures, instructions, and written agreements. Any request to share Data, or Sensitive Personal Data, with non-Agents shall only occur if authorized by the individual in writing.

ERT wird keine Daten oder sensible personenbezogene Daten über Betroffene, Mitarbeiter vor Ort oder Sponsorpersonal an Vertreter weitergeben, es sei denn, diese Parteien sind vertraglich verpflichtet, sich an im Wesentlichen dieselben Programm- und Qualitätsverfahren, Anweisungen und schriftlichen Vereinbarungen zu halten. Jede Anfrage zur Weitergabe von Daten oder sensiblen personenbezogenen Daten an Nicht-Vertreter darf nur erfolgen, wenn sie von der Person schriftlich genehmigt wurde.

Services performed by ERT, in the context of a clinical trial, are subject to ERT's Program requirements, Quality Management program requirements, and applicable Sponsor instructions and written agreements.

Die von ERT im Rahmen einer klinische Studie erbrachten Dienstleistungen unterliegen den Programmanforderungen von ERT, den Anforderungen des Qualitätsmanagement-Programms sowie den geltenden Sponsorenanweisungen und schriftlichen Vereinbarungen.

5.6 Data Protection Measures/Datenschutzmaßnahmen

ERT shall ensure Personnel and Agents (where applicable) comply with the company's Privacy Protection and Data Security measures, in accordance with Program requirements, this Policy, and other applicable data privacy and security laws and regulations.

ERT stellt sicher, dass Personal und Vertreter (falls zutreffend) die Datenschutz- und Datensicherheitsmaßnahmen des Unternehmens in Übereinstimmung mit den Programmanforderungen, dieser Richtlinie und anderen anwendbaren Gesetzen und Vorschriften zum Datenschutz und zur Datensicherheit einhalten.

5.7 Organizational Measures/Organisatorische Maßnahmen

ERT shall ensure that the following measures are taken when Using Data, in accordance with Program Requirements, this Policy, and applicable data privacy and security laws and regulations:

ERT stellt sicher, dass die folgenden Maßnahmen bei der Verwendung von Daten in Übereinstimmung mit den Programmanforderungen, dieser Richtlinie und den geltenden Gesetzen und Vorschriften zum Datenschutz und zur Datensicherheit ergriffen werden:

- Personnel and Agents (where applicable) shall be made aware of Program requirements and shall be provided with a copy of this Policy, where necessary.
- Das Personal und die Vertreter (falls zutreffend) sind auf die Programmanforderungen hinzuweisen und erhalten gegebenenfalls eine Kopie dieser Richtlinie.
- Only those Personnel and Agents (where applicable) shall be authorized to Use Data in order to carry out the assigned duties.
- Nur das Personal und die Vertreter (falls zutreffend) sind berechtigt, die Daten zur Erfüllung der zugewiesenen Aufgaben zu verwenden.
- Personnel and Agents Using Data will be appropriately trained and supervised to ensure compliance with Program
- Personal und Vertreter, die Daten verwenden, werden entsprechend geschult und überwacht, um die Einhaltung der Programmanforderungen und der

requirements and applicable data privacy and security laws and regulations.

- Data Use shall be periodically reviewed to ensure compliance with Program requirements, this Policy, and applicable data privacy and security laws and regulations.

geltenden Datenschutzgesetze und –vorschriften sicherzustellen.

- Die Datennutzung wird regelmäßig überprüft, um die Einhaltung der Programmanforderungen, dieser Richtlinie und der geltenden Datenschutzgesetze und -vorschriften sicherzustellen.

ERT shall periodically evaluate (and review) Personnel and Agent performance to ensure compliance with Program requirements, and this Policy, in accordance with applicable data privacy and security laws and regulations.

ERT bewertet (und überprüft) regelmäßig die Leistung des Personals und des Vertreters, um die Einhaltung der Programmanforderungen und dieser Richtlinie in Übereinstimmung mit den geltenden Gesetzen und Vorschriften zum Datenschutz und zur Datensicherheit sicherzustellen.

5.8 Data Transfers/Datenübertragungen

ERT shall ensure Data transfers (including making Data available remotely) outside the European Economic Area, and Switzerland, are performed in compliance with Program requirements, applicable data privacy and security laws and regulations, in conformance with Privacy Shield principles or the EU standard contractual clauses, where required. Such transfers are carried out only to perform the applicable services required of ERT or its Agents (where applicable) and Subjects, Patients, and Personnel have consented to the transfers, where required.

ERT stellt sicher, dass Datenübertragungen (einschließlich Fernzugriff auf Daten) außerhalb des Europäischen Wirtschaftsraums und der Schweiz in Übereinstimmung mit den Programmanforderungen, geltenden Gesetzen und Vorschriften zum Datenschutz und zur Datensicherheit, gegebenenfalls in Übereinstimmung mit den Privacy Shield-Grundsätzen oder den EU-Standardvertragsklauseln durchgeführt werden. Solche Übertragungen werden nur durchgeführt, um die anwendbaren Dienstleistungen zu erbringen, die von ERT oder seinen Vertretern (falls zutreffend) verlangt werden, und die Personen, Patienten und Mitarbeiter haben den Übertragungen, falls erforderlich, zugestimmt.

5.9 Unauthorized Disclosure, Data Breach, and Security Incident/Unbefugter Offenlegungs-, Datenverletzungs- und Sicherheitsvorfall

ERT shall ensure that if any Personnel and Agents (where applicable) become aware of any potential or identified Unauthorized Disclosure, Data Breach, or Security Incident,

ERT stellt sicher, dass Mitarbeiter und Beauftragte (falls zutreffend) von möglichen oder festgestellten unbefugten Offenlegungen, Datenschutzverletzungen

then such incidents are reported timely, in accordance with Program requirements and applicable data privacy and security laws and regulations.

oder Sicherheits-vorfällen Kenntnis erlangen, wobei diese Vorfälle in Übereinstimmung mit den Programmanforderungen und den geltenden Gesetzen und Vorschriften zum Datenschutz und zur Datensicherheit rechtzeitig gemeldet werden.

5.10 Training/ Training

ERT shall ensure its Personnel, who are required to Use Data to fulfill business services and operations, complete data privacy and security training within 90 days of new-hire on-boarding and annually thereafter.

ERT stellt sicher, dass ihr Personal, das verpflichtet ist, Daten zur Erfüllung von Geschäftsdienstleistungen und -abläufen zu verwenden, innerhalb von 90 Tagen nach der Einstellung im Unternehmen und danach jährlich Datenschutz- und Sicherheitstrainings absolviert.

ERT shall ensure its Agents, who are required to Use Data to fulfill business services and operations, on ERT's behalf complete data privacy and security training before any services begin.

ERT stellt sicher, dass seine Vertreter, die verpflichtet sind, Daten zur Erfüllung von Unternehmensdienstleistungen und -betrieben zu verwenden, im Namen von ERT vor Beginn der Dienstleistungen eine vollständige Datenschutz- und Sicherheitsschulung durch-laufen.

5.11 Privacy Shield Frameworks/ Privacy Shield Frameworks

ERT complies with the EU-US and Swiss-US Privacy Shield Frameworks, as set forth by the US Department of Commerce, regarding Data collection, use, and retention from European Union member countries and Switzerland. ERT adheres to the Privacy Shield Principles of Notice, Choice, and Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, Recourse, Enforcement, and Liability. To learn more about the Privacy Shield program, and to view our certification page, visit https://www.privacyshield.gov/.

ERT hält sich an die EU-US und Swiss-US Privacy Shield Frameworks des US-Handelsministeriums bezüglich der Daten-erfassung, -verwendung und -speicherung durch Mitgliedsländer der Europäischen Union und der Schweiz. ERT hält die Privacy Shield Principles in Bezug auf Benachrichtigung, Wahlmöglichkeit, Verantwortlichkeit für Weiterleitung, Sicherheit, Datenintegrität und Zweckbindung, Zugriff und Rückgriff, Durchsetzung und Haftung ein. Um mehr über das Privacy Shield-Programm zu erfahren und unsere Zertifizierungsseite aufzurufen, besuchen Sie bitte https://www.privacyshield.gov/

For Data transferred under the Privacy Shield Frameworks, ERT is subject to the

Bei Daten, die im Rahmen der Privacy Shield Frameworks übertragen werden, unterliegt

investigatory and enforcement authority of the Federal Trade Commission.

Under the Privacy Shield Frameworks, ERT shall comply with the requirements to notify EU and Swiss individuals whose Data is transferred into the United States, ensuring that the following requirements are satisfied:

- Individuals have the right to access their Data. EU and Swiss individuals wishing to do so may submit a subject access request to privacy@ert.com and such request will be managed in accordance with ERT's SOP-123 Subject Access Request.

- EU and Swiss individuals' Data may be shared in response to lawful requests by public authorities, including to meet national security and law enforcement requirements.

- ERT is liable for the onward transfer of EU and Swiss individual Data to Agents (where applicable), in accordance with applicable service agreements, unless ERT can prove it was not a party to the actions giving rise to the damages.

In compliance with the Privacy Shield Principles, ERT commits to resolve complaints about individuals' privacy and ERT's Use of your Data transferred to the United States under the Privacy Shield. European Union and Swiss individuals with Privacy Shield inquiries or complaints should first contact ERT at privacy@ert.com.

ERT der Untersuchungs- und Vollstreckungsbehörde der Federal Trade Commission.

Im Rahmen der Privacy Shield Frameworks muss ERT die Anforderungen erfüllen, Personen aus der EU und der Schweiz, deren Daten in die Vereinigten Staaten übertragen werden, zu informieren und sicherzustellen, dass die folgenden Anforderungen erfüllt werden:

- Personen haben das Recht, auf ihre Daten zuzugreifen. Personen aus der EU und der Schweiz, die dies wünschen, können einen Antrag auf Zugang an privacy@ert.com stellen. Dieser Antrag wird in Übereinstimmung mit ERT SOP-123 bearbeitet.
- Die Daten von Personen aus der EU und der Schweiz können auf rechtmäßige Anfragen von Behörden hin weitergegeben werden, auch um die nationalen Sicherheits- und Strafverfolgungsanforderungen zu erfüllen.
- ERT haftet für die Weiterleitung von EU- und schweizerischen Einzeldaten an Vertreter (falls zutreffend) gemäß den geltenden Dienstleistungsverträgen, es sei denn, ERT kann nachweisen, dass ERT nicht an den schadensverursachenden Maßnahmen beteiligt war.

In Übereinstimmung mit den Datenschutzgrundsätzen verpflichtet sich ERT, Beschwerdefälle über die Privatsphäre von Personen und die Nutzung der im Rahmen des Datenschutzes in die Vereinigten Staaten übermittelten Daten durch ERT zu lösen. Personen aus der Europäischen Union und der Schweiz, die Fragen oder Beschwerden zu dieser Datenschutzerklärung haben, sollten sich zunächst an ERT wenden privacy@ert.com.

ERT has further committed to refer unresolved privacy complaints (under the Privacy Shield Principles) to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint or if your complaint is not satisfactorily addressed, visit www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

ERT hat sich ferner verpflichtet, ungelöste Datenschutzbeschwerdefälle (gemäß den Privacy Shield Principles) an einen unabhängigen Streitbeilegungsmechanismus, den BBB EU PRIVACY SHIELD, zu verweisen, der vom Council of Better Business Bureaus betrieben wird. Wenn Sie keine fristgerechte Bestätigung Ihrer Be-schwerde erhalten oder wenn Ihre Be-schwerde nicht zufriedenstellend behandelt wird, besuchen Sie www.bbb.org/EU-privacy-shield/for-eu-consumers/ für weitere Informati-onen und um eine Beschwerde einzureichen, Dieser Service ist für Sie kostenlos.

If your complaint involves Personnel Data transferred to the United States from the EU or Switzerland in the context of the employment relationship and ERT does not address it satisfactorily, ERT commits to cooperate with the panel established by the EU data protection authorities ("DPA Panel") (or the Swiss Federal Data Protection and Information Commissioner, as applicable) and to comply with the advice given by the DPA Panel (or Commissioner, as applicable) with regard to such Personnel Data. To pursue an unresolved Personnel complaint, individuals should contact the state or national data protection or labor authority in the appropriate jurisdiction. Complaints related to Personnel Data should not be addressed to the BBB EU PRIVACY SHIELD.

Betrifft Ihre Beschwerde Personaldaten, die im Rahmen des Arbeitsverhältnisses aus der EU oder der Schweiz in die Vereinigten Staaten übermittelt werden, und ERT geht nicht zufriedenstellend darauf ein, verpflichtet sich ERT, mit dem von den EU-Datenschutzbehörden ("DPA-Panel") (oder gegebenenfalls dem Eidgenössischen Datenschutz- und Informationskommissar) eingerichteten Panel zusammenzuarbeiten und den Empfehlungen des DPA-Panels (oder gegebenenfalls des Kommissars) in Bezug auf diese Personaldaten nachzukommen. Um eine ungelöste Personalbeschwerde einzureichen, sollten sich Einzelpersonen an die staatliche oder nationale Datenschutz- oder Arbeitsbehörde der jeweiligen Gerichtsbarkeit wenden. Beschwerden im Zusammenhang mit Personaldaten sollten nicht an die BBB EU PRIVACY SHIELD gerichtet werden.

Contact details for the EU data protection authorities can be found at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

Die Kontaktdaten der EU-Datenschutzbehörden finden Sie unter http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

Contact details for the Swiss Federal Data Protection and Information Commissioner can be found at https://www.edoeb.admin.ch/edoeb/en/home/

Die Kontaktdaten des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten finden Sie unter https://www.edoeb.admin.ch/edoeb/en/home/

the-fdpic/links/data-protection---switzerland.html

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, individuals may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. Refer to the Privacy Shield Annex 1 https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

the-fdpic/links/data-protection---switzerland.html.

Wenn Ihre Privacy Shield-Beschwerde nicht über die oben genannten Kanäle gelöst werden kann, können Einzelpersonen unter bestimmten Bedingungen ein bindendes Schiedsverfahren für einige verbleibende Ansprüche einleiten, die nicht durch andere Rechtsbehelfe gelöst wurden. Siehe Anhang 1 zum Privacy Shield unter https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

5.12 Corrective Actions/Korrekturmaßnahmen

ERT shall ensure that appropriate steps are taken to comply with Program requirements, this Policy, and applicable data privacy and security regulations for maintaining Data confidentiality. Any violation of Program requirements, this Policy, or other applicable data privacy and security regulations by Personnel (or Agents, where applicable) shall be grounds for corrective action, up to, and including termination or revocation of the applicable service agreement.

ERT stellt sicher, dass geeignete Maßnahmen ergriffen werden, um die Programmanforderungen, diese Richtlinie und die geltenden Datenschutz- und Sicherheitsvorschriften zur Wahrung der Vertraulichkeit der Daten einzuhalten. Jeder Verstoß gegen die Programmanforderungen, diese Richtlinie oder andere anwendbare Datenschutz- und Sicherheitsvorschriften durch Personal (oder Vertreter, falls zutreffend) ist Grund für Korrekturmaßnahmen, bis hin zur Kündigung oder zum Widerruf des betreffenden Servicevertrags.

5.13 Audit/Audit

ERT shall ensure Program requirements, identified herein, are routinely audited by Quality Management, or the DPO, (or outside auditor, where required) no less than once annually to ensure compliance with applicable data privacy and security laws and regulations.

ERT stellt sicher, dass die hierin genannten Programmanforderungen routinemäßig vom Qualitätsmanagement, dem DPO (oder, falls erforderlich, von einem externen Auditor) mindestens einmal jährlich überprüft werden, um die Einhaltung der geltenden Gesetze und Vorschriften zum Datenschutz und zur Datensicherheit sicherzustellen.

5.14 Data Risk Classification Chart/Daten-Risikoklassifizierungsdiagramm Ebene

	Data Type/ Datentyp	Risk Classification/ Risikoklassifizierung	Data Examples/ Datenbeispiele
Critical **Kritisch**	Subject/Patient Clinical Trial Data Daten der betroffenen Person/Patientendaten der klinischen Studie	**Restricted Data** Data that would cause severe harm to individuals and/or ERT if disclosed. Controls strictly limit the ability to use this information including no ability to extract for operational purposes, unless authorized in writing by ERT Management. **Eingeschränkte Daten** Daten, die bei einer Weitergabe schweren Schaden für Personen und/oder ERT verursachen würden. Kontrollen schränken die Möglichkeit der Nutzung dieser Informationen streng ein, einschließlich der Möglichkeit, sie für betriebliche Zwecke zu extrahieren, es sei denn, das ERT-Management hat dies schriftlich genehmigt.	• Social Security Numbers in association with protected health information or personally identifiable information. Certain individually identifiable medical records and genetic information. • Specific contractual or customer obligations. • Research information classified as highly restricted use. • Sozialversicherungsnummern in Verbindung mit geschützten Gesundheitsinformationen oder persönlich identifizierbaren Informationen. Bestimmte individuell identifizierbare medizinische Aufzeichnungen und genetische Informationen. • Spezifische vertragliche oder kundenbezogene Verpflichtungen • Forschungsinformationen, die als stark eingeschränkte Nutzung eingestuft werden
High Hoch	ERT Employee Data; Client personnel Data; and Vendor personnel Data	**Private Data** Data that would likely cause harm to individuals and/or ERT if disclosed.	• Protected Health Information • Personally Identifiable Information including

	Data Type/ Datentyp	Risk Classification/ Risikoklassifizierung	Data Examples/ Datenbeispiele
	ERT-Mitarbeiterdaten, Kundenpersonaldaten und Lieferantenpersonal-daten	Controls limit access but allow information to be extracted and accessed for business operational purposes. **Persönliche Daten** Daten, die bei einer Weitergabe wahrschein-lich einen Schaden für Personen und/oder ERT verursachen würden. Kontrollen schränken den Zugriff ein, ermög-lichen aber die Extrak-tion und den Zugriff auf Informationen für geschäftliche betrieb-liche Zwecke.	Social Security Number and National ID • Financial Records including banking information for direct deposit • Employee credentials. • Business email address and telephone number • CVs • Passwords that can be used to access confidential information • Geschützte Gesundheitsinformatio-nen • Persönlich identifi-zierbare Informationen, einschließlich Sozial-versicherungsnummer und National ID • Finanzunterlagen, einschließlich Bank-informationen für direkte Einzahlungen • Anmeldedaten der Mitarbeiter. • Geschäfts-E-Mail-Adresse und Telefon-nummer • CVs • Passwörter, die für den Zugriff auf vertrauliche Informationen verwendet werden können.
Medium Mittel	ERT Confidential Information	**Proprietary Data** Data which would not cause harm if disclosed,	• Policies and Procedures

	Data Type/ Datentyp	Risk Classification/ Risikoklassifizierung	Data Examples/ Datenbeispiele
	Vertrauliche ERT Informationen	but ERT has chosen to keep confidential. Controls allow access with little technical barriers. **Proprietäre Daten** Daten, die bei einer Weitergabe keinen Schaden anrichten würden, ERT sich jedoch für die Geheimhaltung entschieden hat. Kontrollen ermöglichen den Zugang mit wenig technischen Barrieren.	• ERT's financial and accounting records • Training materials • Press Statements • Audit reports • Richtlinien und Verfahren • Die Finanz- und Buchhaltungsunterlagen von ERT • Schulungsunterlagen • Pressemitteilungen • Auditberichte
Low Niedrig	ERT Corporate Website ERT Corporate Website	**Public Data** Data that is readily accessible to the general public and not received or disclosed by ERT. **Öffentliche Daten** Daten, die für die breite Öffentlichkeit leicht zugänglich sind und vom ERT nicht empfangen oder weitergegeben wurden.	• Social media profiles (e.g., LinkedIn, Facebook, Twitter, etc.) • Online address directories (e.g., White Pages) • Social Media Profile (z.B. LinkedIn, Facebook, Twitter, etc.) • Online-Adressverzeichnisse, z.B. White Pages

6. Record Retention/Aufbewahrungsdauer

All documents (electronic or hard copy) produced as a result of the process outlined within this policy shall be retained in accordance with, POL COR-004 Record Retention Policy.

Alle Dokumente (elektronisch oder in Papierform), die als Ergebnis des in dieser Richtlinie beschriebenen Prozesses erstellt wurden, werden in Übereinstimmung mit POL COR-004 Richtlinie zur Aufbewahrung von Aufzeichnungen aufbewahrt.

7. Revision History/Revisionshistorie

Version/ Version	Date/ Datum	Author/ Autor	Changes/ Änderungen	
5	15JAN2011	Richard Miller	• Minor updates to include the Höchberg, Germany Office. • Applied new Policy Format in accordance with revised SOP 112 – Format and Preparation/Revision of Standard Operating Procedures, Standard Work Instructions and Policies. • Added clarification regarding compliance with Safe Harbor principles.	• Kleine Updates um das Büro in Höchberg, Deutschland einzuschließen. • Angewandtes neues Richtlinienformat in Übereinstimmung mit der überarbeiteten SOP 112 - Format und Erstellung/ Überarbeitung der Standard Operating Procedures Standard Work Instructions und Richtlinien. • Zusätzliche Klarstellung zur Einhaltung der Safe Harbor-Grundsätze.
6	27FEB2012	Richard Miller	• Updated to accommodate HR data transfers out of the EU to ERT Corporate facilities in Philadelphia, PA USA. • Updated to specifically identify U.S.-Swiss Safe Harbor Framework for inclusion.	• Aktualisiert, um die Übermittlung von Personaldaten aus der EU an ERT Corporate Standorte in Philadelphia, PA USA, zu ermöglichen. • Aktualisiert, um den U.S.-Swiss Safe Harbor Framework für die Aufnahme speziell zu identifizieren.
7	25NOV2013	Richard Miller	• Revised the Personal/Clinical Information definition to include encoded or	• Die Definition der persönlichen/klinischen Informationen wurde überarbeitet, um verschlüsselte

Version/ Version	Date/ Datum	Author/ Autor	Changes/ Änderungen	
			anonymized information.	oder anonymisierte Informationen aufzunehmen.
8	16SEP2016	Stephen Raymond	• Expanded scope to ensure that this policy document is the master document for ERT privacy and integrity. • Changed title to include information integrity. • Added references essential to carrying out this policy: Security issue, breach reporting, HIPAA policy, Privacy Shield Certification. • Specified the regulations and guidance documents that this Policy explicitly conforms. • Added reporting and breach notification reference • Applied the necessary modifications for compliance with the BBB and U.S.	• Erweiterter Geltungsbereich, um sicherzustellen, dass dieses Richtliniendokument das Masterdokument für den Datenschutz und die Integrität des ERT ist. • Titel geändert, um die Informationsintegrität aufzunehmen. • Zusätzliche Hinweise, die für die Durchführung dieser Richtlinie unerlässlich sind: Sicherheitspro-blem, Meldung von Verstößen, HIPAA-Richtlinie, Privacy Shield Zertifizierung. • Vorschriften und Leitfäden spezifiziert, die diese Richtlinie ausdrücklich einhält. • Berichterstattung und Verweis auf Benachrichtigungen über Verstöße hinzugefügt. • Die notwendigen Anpassungen zur Einhaltung der BBB und des USA Handelsministeriums

Version/ Version	Date/ Datum	Author/ Autor	Changes/ Änderungen	
			Department of Commerce.	wurden vorgenommen
9	10JUL2017	Richard Miller	• Revised to accurately reflect the changes required to support the US-Swiss Privacy Shield Framework. References to the SwissSafe Harbor have been removed.	• Überarbeitet, um die Änderungen, die zur Unterstützung des US-amerikanischen Privacy Shield Framework erforderlich sind, korrekt wiederzugeben. Verweise auf den SwissSafe Harbor wurden entfernt.
10	05JUN2018	Mark Wright	• Revised to include references to GDPR.	• Überarbeitet, um Verweise auf DSGVO aufzunehmen.
11	28FEB2019	Veronica Contreras	• Revised overall policy to align with company Program requirements. • Converted the document to the new Bilingual Policy Template TMPL 112_04, which includes both the English and the German-translated content.	• Gesamtstrategie zur Anpassung an die Anforderungen des Unternehmensprogramms überarbeitet. • Das Dokument wurde in die neue zweisprachige Richtlinienvorlage TMPL 112_04 konvertiert, die sowohl den englischen als auch den deutsch übersetz -ten Inhalt enthält.
12	04OCT2019	Veronica Contreras	• Update definition of Data. • Added reference to APPI. • Added definition of unauthorized disclosure.	• Aktualisieren der Definition von Daten. • Verweis auf APPI hinzugefügt. • Definition der nicht autorisierten Offenlegung hinzugefügt.

Version/ Version	Date/ Datum	Author/ Autor	Changes/ Änderungen	
			• Updated Program pyramid to ensure document names were updated, where required. • Correct formatting and wording throughout the document.	• Die Programmpyramide wurde aktualisiert, um sicherzustellen, dass die Dokumentnamen bei Bedarf aktualisiert wurden. • Korrekte Formatierung und Formulierung im gesamten Dokument.