



## Open Research Data Depository

**Deliverable:** D7.2 Open Research Data Depository

**Author:** Florence Blandinieres

**Version:** 1.0

**Quality review:** Georg Licht

**Date:** 07 August, 2017

**Grant Agreement number:** 727073

**Starting Date:** 01/04/2017

**Duration:** 24 months

**Coordinator:** Dr. Georg Licht, ZEW

**Email:** licht@zew.de



---

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Data sources and related rights</b>	<b>2</b>
2.1	Replication of results: R&D parameters . . . . .	2
2.2	Replication of results: adoption parameters . . . . .	2
<b>3</b>	<b>Diffusing results and practices</b>	<b>3</b>
<b>4</b>	<b>Concluding remarks</b>	<b>3</b>
<b>A</b>	<b>Exclusive license for using Fraunhofer data for FRAME</b>	<b>4</b>
<b>B</b>	<b>Data Protection</b>	<b>14</b>

## 1 Introduction

The current report presents the main infrastructure which will be developed to allow the general use of the FRAME data and scripts. In line with the ongoing debate about Open Science, the research data depository aims at making possible for third parties to access, to mine, to exploit, to reproduce, and to disseminate results without additional costs. The main results and description of the variables will be disclosed in scientific peer-reviewed articles.

## 2 Data sources and related rights

Different types of data are crossed within the Work Package 6 for the estimation of the calibrated parameters used across the work packages. Four main different databases are involved which combine several sources of information: 1/ a panel dataset covering different countries and technologies which differentiates between public and private patents, 2/ a matched German CIS-Fraunhofer panel dataset, 3/ the European CIS datasets, and 4/ a matched US defense patents R&D. The results of the core estimations from the Work Package 6 will be available on the website. The consortium will hold the rights on the datasets 1 and 4, the latter being based on different public sources. The right on the dataset 3 is held by Eurostat who allows scientific licenses to conduct scientific research. Only the dataset 2 which belongs to the Fraunhofer Society is confidential and therefore cannot lead to the disclosure of the contents (see appendix for the related letter about the use of proprietary data and FRAME).

### 2.1 Replication of results: R&D parameters

To facilitate the uptake of the project, FRAME will ensure the maximum of transparency in order to replicate results. To do so, efforts will be made to ensure the public disclosure of the scripts (see next section) and the access to the datasets involved, unless specific confidentiality requirements prevent it. In this regard, most of the datasets should be accessible for replication studies and training purposes. The first set of parameters estimated relates to R&D parameters. The latter are estimated based on national statistical offices, EUROSTAT, Patstat data. The matching procedure used on Patstat to delineate sectors and countries will be made available for replication. The consortium cannot allow to publish data at the micro-level due to the fees and the licenses related to the use of the data, collected, and maintained by European Patent Office. The consortium will provide access to patent data at aggregated levels (e.g. sectors and countries) and will be available within the ZEW Data Research Center. Information to proceed will be available on the FRAME website. The other sources of information involved will be available through the national statistical offices websites.

### 2.2 Replication of results: adoption parameters

The estimation of the adoption parameters relies on various existing datasets: the CHAT dataset, the Government Budget Appropriation Of Research and Development (GBAORD) data, and the result of a matching procedure between German CIS data and the Fraunhofer data. The two first sources of data is already publicly accesible: the CHAT dataset is downloadable from <http://graduateinstitute.ch/fr/home/study/academicdepartments/international-economics/md4stata/datasets/chat.html> and described in <http://www.nber.org/papers/w15319>. In the same vein, the use of governmental data is publicly available [2](http://ec.europa.eu/eurostat/statistics-</a></p></div><div data-bbox=)

`explained/index.php/R_%26_D_expenditure`. Only the data coming from confidential contracts between Fraunhofer institutes and firms will not be available for replication. The datasets contains the research contracts signed between the Fraunhofer Society and German firms for more than 20 years. Fraunhofer Society consists of one of the largest applied research organization in Europe and hence, represents a large portion of German public research disseminated among German firms. Combined with the CIS data, the sample represents around 50,000 identified firms collaborating with Fraunhofer institutes. Considering the confidential nature of the data, the consortium could get access to the data only for estimating the parameters without additional allowance to publish the contents of the dataset (see the specific and restricted allowance of the Fraunhofer Society to conduct the FRAME project in appendix A). Finally, the robustness checks with defense patents will also involve Patstat data and could be available for replication at an aggregated level.

### 3 Diffusing results and practices

In order to allow the use of the models by third parties, to exploit new insights, or to extend the models, the scripts involved in each Work Package will be available on the website. If necessary, a depository will be created on GITHUB and added on the website. The software programs used to code the different models are widely spread among the scientific community (Stata, R, Matlab, Dynare, GAUSS) and provides the maximum of transparency. Doing so will pave the ground for reproducibility of the findings and potential extensions. One exception will be the algorithm (“search engine”) developed in ZEW in order to match patent data with large firms databases.

Different types of workshops, summer schools, and training seminars will be created to diffuse the use of the model. The first workshop to introduce the features of the model is scheduled for the 13th of September. The meeting will take place in Brussels at the initiative of the DG RTD unit and combined with the MONROE project. Regarding the publication of the results, we will try to ensure that the maximum of publications will follow the “gold open access” rule by sending them to open access journals. In the case that journals do not follow this logic, we will apply a “green open access”: in line with the requirements of the Horizon 2020, researchers will ensure that the related articles will be openly available and free of costs. Working Papers depositories of each institution involved in the FRAME project will be also be considered to accelerate the speed of diffusion of the findings (“green open access”). The links towards each working paper depository will be made through the website.

### 4 Concluding remarks

The information generated before the beginning of the project will remain the property of the partner. The main result of the project will be owned by the partner who carried out the majority of the work leading to such results. In case of joint foreground related to the collaboration between several partners from the consortium, the latter will have a joint co-ownership of the findings and an agreement reflecting this will be drawn up between them. This agreement will be checked by the external Scientific Advisory Board. More details will be provided in the Data Management Plan.

**A Exclusive license for using Fraunhofer data for FRAME**

Alex C



## Non Disclosure Agreement

Between

**ZEW, Zentrum für Europäische Wirtschaftsforschung GmbH**  
L7, | 68161 Mannheim,

- hereinafter referred to as »ZEW« -

**Prof. Diego Comin,**  
Professor of Economics, Dartmouth College, 6106 Rockefeller Hall, Hannover, NH 03755-3514, U.S.A.

- hereinafter referred to as »Prof. Comin« -

and

**CIRCLE, Lund University,**  
P.O.Box 117, 22100 Lund, Sweden

- hereinafter referred to as »CIRCLE« -

and

**Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.,**  
Hansastraße 27 c, D-80686 München, Federal Republic of Germany

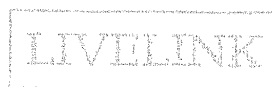
- hereinafter referred to as »Fraunhofer« -

as legal entity for

**Fraunhofer Institut für System- und Innovationsforschung,**  
Breslauer Straße 48, 76139 Karlsruhe

- hereinafter referred to as »Fhl« -

WHEREAS, all Parties, for their mutual benefit and with the purpose of identifying areas of common interest for joint collaborative activities, e.g. in the form of a joint research project to estimate the impact that collaborating with Fraunhofer has on the performance of German



ccy

companies (hereafter referred to as the "Fraunhofer Impact Study"), are desirous to disclose to each other certain business and technical information and data in the following scientific fields:

- 1 data evaluation, data matching and data analysing
- 2 setting up a longitudinal database that combines information on the firms with information on the extent and timing of their collaboration with Fraunhofer

and

In order to define the nature and content of the collaboration regarding the Fraunhofer Impact Study the Parties hereto may wish to exchange technical and/or business information and data of a confidential nature presently in their possession and wish to ensure that the same remain confidential.

Now, therefore, in anticipation of receipt of such information, the Parties agree to the rights, obligations and proprietary information as set forth below:

## 1 Definition of Confidential Information

- 1.1 For the purpose of this Agreement "Disclosing Parties" are: ZEW, Fraunhofer, Fhl and Prof. Comln. This Agreement shall cover Confidential Information disclosed by any party.
- 1.2 The Parties hereto may exchange proprietary information including but not limited to technical, business, performance, sales, financial and contractual information, documents and data (hereinafter referred to as "Confidential Information"). "Confidential Information" as used herein shall mean all information which is: (a) communicated by one party to the other party in written or tangible form, and (b) orally communicated by one party to the other party, and confirmed in writing within fourteen (14) days after such oral disclosure. The fact that the parties have entered into this Agreement, or that there is a relationship between the parties, is Confidential Information.
- 1.3 The restrictions on the use and disclosure of Confidential Information shall not apply to any information which is:
  - (a) proven to have been known to the receiving party prior to the time of its receipt pursuant to this Agreement; or
  - (b) in the public domain at the time of disclosure to the receiving party or thereafter enters the public domain without breach of the terms of this Agreement; or

A handwritten signature in black ink, appearing to be 'G. G. G.', is located in the bottom right corner of the page.

- (c) lawfully acquired by the receiving party from an independent source having a bona fide right to disclose the same; or
- (d) independently developed by an employee of the receiving party who has not had access to any of the Confidential Information of the disclosing party.

## 2. Nondisclosure and Nonuse Obligation

- 2.1 The parties each undertake to treat as confidential all and any Confidential Information received and use such Confidential Information only for the purpose of this Agreement and agree not to disclose the same to any third party except with the prior written consent of the disclosing party.
- 2.2 Unless it is necessary for the definition of the collaboration and provided that any copy of Confidential Information is distributed to employees only who have a need to know, the receiving party shall not, without the prior written consent of the disclosing party, copy or reproduce any document provided to the receiving party containing in whole or in part Confidential Information and any party receiving any such document shall return or destroy the same and any copies thereof on the supplying party's request but the latest until termination of this Agreement. This shall not apply to copies of the electronically exchanged Confidential Information made as a matter of routine information technology back-up and to Confidential Information or copies thereof which must be stored by the receiving party according to mandatory law.
- 2.3 All Confidential Information supplied pursuant to this Agreement shall remain the property of the party disclosing or supplying the same and no rights, including but not limited to the right to apply for industrial property rights, are granted to the receiving party in the same.
- 2.4 The act of the disclosing party in conveying Confidential Information to the receiving party shall not be an expressed or implied grant of a license to the receiving party to use any Confidential Information, nor shall it be a grant of a license under any trademark, patent or copyright, or for applications which are now or may hereafter be owned by the disclosing party.

## 3. Permitted Use

A handwritten signature in black ink, appearing to be 'Aly', is written over the page number.



- 3.1 Confidential Information shall be made available by the receiving party only to those employees within their company with a need to know the Confidential Information for the Purpose of this Agreement (hereafter the "Permitted Persons").
- 3.2 In allowing use of the Confidential Information by any Permitted Person in accordance with the provision of Article 3.1, the receiving Party shall ensure that the Permitted Person is bound by confidentiality obligations consistent with this Agreement, that he/she has the duty to exercise his/her best efforts to prevent disclosure of the Confidential Information. The receiving Party shall take appropriate steps to enforce the obligations of Permitted Persons in relation thereto.

#### 4. Designated Representative

The designated representatives of each Party to receive and control Confidential Information exchanged hereunder are listed on end of NDA (Attachment A).

#### 5. Period of the Agreement and Protection Obligation

- 5.1 This Agreement shall come into effect on the date of its signature and remain effective until the earlier of (i) receipt by a party of written notice given by the other party in its sole discretion of its intention to terminate or abandon further negotiations regarding the Fraunhofer Impact Study, or (ii) the execution of a separate agreement for a joint activity by both parties, as far as the Confidential Information falls into the scope of this joint activity, or (iii) 2 calendar years from the effective date of this Agreement, unless extended by written, mutual agreement signed by authorized representatives of the parties.
- 5.2 The obligations to maintain the confidentiality of the Confidential Information provided hereunder shall survive the expiration or termination of this Agreement for a period of 10 years.

#### 6. Injunctive Relief

In case the receiving Party or its employee uses the Confidential Information against the Purpose of this Agreement or releases the Information to any third party, this act

A handwritten signature in black ink, appearing to be 'Aly', is written over the page number.

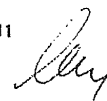
shall be recognized as a serious violation of this Agreement. The parties agree that the unauthorized disclosure or use of Confidential Information of the Disclosing Party could cause irreparable harm and significant injury to such party and that money damages would not be a sufficient remedy for any breach of this Agreement. Upon any actual or threatened violation of this Agreement by the other party, the Disclosing Party shall be entitled, without the obligation to post any bond, to preliminary and permanent Injunctive relief against such violation, in addition to any other rights or remedies which such party may have at law or in equity.

## 7. No Warranty

All Confidential Information is provided "AS IS" and none of such Confidential Information which may be submitted or exchanged by the parties shall constitute any representation, warranty, assurance, guarantee or inducement by either party to the other regarding such Confidential Information's accuracy, completeness or performance and with respect to the infringement of Intellectual Properties or any right of privacy or other rights of any third party.

## 8. General Provisions

- 8.1 This Agreement shall be governed by the laws of the Federal Republic of Germany .
- 8.2 No amendment or modification of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.
- 8.3 Neither this Agreement nor any right or obligation hereunder is assignable in whole or in part by any party without the prior written consent of the other party.
- 8.4 This Agreement constitutes the entire understanding between the parties hereto and supersedes all previous communications, representations, and understanding, oral or written, between the parties with respect to the subject matter of this Agreement. Neither this Agreement nor the disclosure or receipt of Confidential Information shall constitute or imply any promise or intention to make any purchase of products or services by either party.


A handwritten signature in black ink, appearing to be 'Ally', is written over the page number.


8.5 If any provision of this Agreement is determined to be illegal or in conflict with the applicable law, the validity of the remaining provisions shall not be affected. The ineffective provision shall be replaced by an effective provision which is economically equivalent. The same shall apply in case of a gap.

A handwritten signature in black ink, appearing to be 'Duy', is located in the bottom right corner of the page.

IN WITNESS THEREOF, the parties have executed this Agreement on the respective dates entered below. Each research institute or research department of the Parties participating in the exchange of information in the meaning of this Agreement shall respectively receive a simple copy of the original signed Agreement.

Mannheim, January 21<sup>st</sup>, 2015, signed on behalf of ZEW:

  
\_\_\_\_\_  
Prof. Dr. Clemens Fuest,  
President

  
\_\_\_\_\_  
Thomas Kohl  
Director

Date, signed on behalf of Prof. Comin:

\_\_\_\_\_  
Prof. Diego Comin  
Department of Economics  
Dartmouth College

Date, signed on behalf of CIRCLE, Lund University

\_\_\_\_\_  
Prof. Torben Schubert  
Assoc. Professor in Innovation Economics

Date, signed on behalf of Fraunhofer/ Fhl:

\_\_\_\_\_  
Dr. Roman Götter  
Head of Fraunhofer Academy

\_\_\_\_\_  
Stefanie Mielert  
~~Head of Legal Corporate Governance~~

Dr. Lorenz Kaiser  
Division Director Contracts and Commercialization



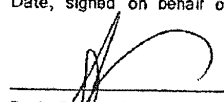
IN WITNESS THEREOF, the parties have executed this Agreement on the respective dates entered below. Each research institute or research department of the Parties participating in the exchange of information in the meaning of this Agreement shall respectively receive a simple copy of the original signed Agreement.

Date, signed on behalf of ZEW:

\_\_\_\_\_  
Prof. Dr. Clemens Fuest,  
President

\_\_\_\_\_  
Thomas Kohl  
Director

Date, signed on behalf of Prof. Comin:

  
\_\_\_\_\_  
Prof. Diego Comin  
Department of Economics  
Dartmouth College

Date, signed on behalf of CIRCLE, Lund University

\_\_\_\_\_  
Prof. Torben Schubert  
Assoc. Professor in Innovation Economics

Date, signed on behalf of Fraunhofer/ FHL:

\_\_\_\_\_  
Dr. Roman Götter  
Head of Fraunhofer Academy

\_\_\_\_\_  
~~Stefanie Mielert~~  
~~Head of Legal Corporate Governance~~

Dr. Lorenz Kaiser  
Division Director Contracts and Commercialization



IN WITNESS THEREOF, the parties have executed this Agreement on the respective dates entered below. Each research institute or research department of the Parties participating in the exchange of information in the meaning of this Agreement shall respectively receive a simple copy of the original signed Agreement.

Date, signed on behalf of **ZEW**:

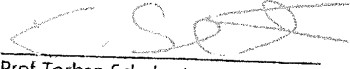
\_\_\_\_\_  
Prof. Dr. Clemens Fuest,  
President

\_\_\_\_\_  
Thomas Kohl  
Director

Date, signed on behalf of **Prof. Comin**:

\_\_\_\_\_  
Prof. Diego Comin  
Department of Economics  
Dartmouth College

Date, signed on behalf of **CIRCLE**, Lund University

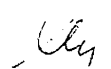
  
\_\_\_\_\_  
Prof. Torben Schubert  
Assoc. Professor in Innovation Economics

Date, signed on behalf of **Fraunhofer/ Fhl**:

\_\_\_\_\_  
Dr. Roman Götter  
Head of Fraunhofer Academy

\_\_\_\_\_  
~~Stefanie Mielert~~  
~~Head of Legal Corporate Governance~~

Dr. Lorenz Kaiser  
Division Director Contracts and Commercialization



## **B Data Protection**

## Data Protection Policy

(Last updated: 1 May 2017)

### 1. Activities, Organisational Structure

ZEW is a non-profit economics research institute with the legal form of a "GmbH". Founded in 1990, the institute is dedicated to conducting economic research, economic policy advising, the academic training of young researchers, and the dissemination of research findings to professionals and the lay public. Under the leadership of Prof. Achim Wambach, PhD, the president of ZEW, and Thomas Kohl, the commercial director of ZEW, the institute currently employs 188 people in six research departments, three research groups and three service departments.

ZEW processes several different types of personal data, including the personal data of employees as part of human resources management; data gathered during the surveying of companies and individuals; data that are collected to host events and training seminars; and data about third-party suppliers.

### 2. Legal Regulations Relevant to the Processing of Personal Data

As a GmbH subject to public law, ZEW must adhere to the requirements of the Federal Data Protection Act (BDSG).

In accordance with Article 4f of the BDSG, ZEW must appoint a Data Protection Officer (Datenschutzbeauftragter). The appointed officer is

Dr. Thomas Wirth, Esq.

ZEW employees who process personal data are required to sign a document binding them to maintain data confidentiality. This obligation to uphold data confidentiality remains in force even after employment at ZEW comes to an end. Specifically, employees are only authorised to process and use personal data within the scope of their professional responsibilities. In the event that external organisations are entrusted with gathering, storing, modifying, using or transferring personal data, then these organisations and/or the involved individuals are required to sign a document binding them to uphold data protection laws as well as maintain data confidentiality.

The BDSG obligates individuals who process data in a legitimate manner to undertake measures to ensure the confidentiality, integrity and availability of said data. These individuals must ensure unauthorised persons do not gain access to data, whether from "without" (by attacking IT systems, breaking into server rooms, or theft) or from "within" (due to lack of data compartmentalisation, insufficient authorisation rights, or similar).

Article 9 of the BDSG in conjunction with the appendix to Article 9, line 1 of the BDSG set forth security measures that are necessary from a technical and organisational perspective. As a "responsible party" pursuant to the BDSG, ZEW undertakes the following data protection measures:



## **Access Monitoring**

Access to the premises of ZEW (L7, 1, 68161 Mannheim, built: 1996) is protected by a camera monitoring system. The executive management grants access authorisation, and reception sets up access rights for each person based on individual requirements. Access rights are regularly reviewed and, as a general rule, are time limited. Reception manages keys and distributes access cards following approval from the executive management. Access to the office areas is protected with electronic locks. Visitors must report to reception, where they are personally received by ZEW employees and escorted through the office areas, which are secured with electronic locks.

There is an emergency action plan for the building, and on weekends the availability of the responsible system administrators is assured.

All data saved by ZEW to IT systems are stored on the servers located in ZEW's server room. Security doors as well as an electronic access system, which can only be opened with an access code, protect the server room itself. Access to this room is only granted to IT system administrators as well as – should an emergency occur – to the building supervisor and fire department. All individuals with access to the server room must pledge to maintain strict data confidentiality.

The servers are located in room 361 on the third floor of the ZEW building.

The terminals that are connected to these servers are located in the offices of the relevant project employees.

The server and terminals are part of a secure network.

## **Access Control**

ZEW's IT network as well as the staff desktop computers with access to data are password protected. The passwords must be at least 8 characters long and they are regularly (every 180 days) changed.

The raw data are saved exclusively on a specific project server in the server room. Data sets are saved in individual folders based on an assigned project number. The project data servers have a special user administration system that is not connected to a directory service. This assures that only individuals identified in contracts have access to the data (other ZEW employees and external service providers have no access). Data backup is assured with a Redundant Array of Independent Servers (RAIS). Once data are deleted, they are fully deleted during the next backup session.

Project employees have access to data via terminals outfitted with special security protocols. Data are not saved on these terminals. All servers and terminals are password protected. The terminals are outfitted with password-protected screensavers. Security guidelines are issued to all project employees in order to instruct them in the correct use of passwords and IT systems.

When an employee leaves a desk, he must lock all workstations with network access. In addition, all workstations have password-protected screensavers that activate automatically when the computer has not been used for 15 minutes.

Access to IT systems is only possible for employees who have been granted authorisation to work on a given project. The IT administrator issues access rights to ZEW's network for the duration of a staff member's employment at ZEW. Granted access rights are reviewed on a regular basis to ensure they are current. When issuing access rights to data sets that are subject to special confidentiality requirements, the IT administrator and project director work in coordination with the Data Protection Officer and hold a special training session in which the employee receiving access must pledge to uphold data confidentiality requirements. Password protection and IP address verification are used to limit access exclusively to project employees. The remote processing of data outside of the institute is not possible from a technical perspective. The servers and terminals are protected by a firewall. The project data servers have no internet connectivity.

ZEW employees can receive remote access to the ZEW network via VPN connection if they make a special request. The VPN access is protected by the employee's token. The token generates a temporary password for every VPN connection. Establishing a VPN connection automatically activates a firewall on the remote computer.

The majority of ZEW employees have portable computers (laptops, notebooks). Access to these computers is also password protected. Portable computers are not used for working with sensitive data.

### **Prevention of Data Sharing**

Sensitive data that are subject to special data protection agreements (e.g. micro datasets containing personal and firm data) remain on ZEW's network server and are not stored or saved locally. Data obtained externally are saved on the project data server. Only the relevant project employees and system administrators have access to this server. In addition, IT employees only access the server to perform technical maintenance or data backups. All staff, including external service providers who regularly work at ZEW, receive instruction and must take a pledge in accordance with Art. 5 of the Federal Data Protection Act. ZEW servers and terminals are protected by a firewall.

Project data servers that store particularly sensitive data have no internet or VPN connectivity, and also lack an electronic signature. Due to the structure of the network, encryption is not necessary. Wireless internet (WiFi) is not used.

Data storage devices that are given to ZEW by individuals or organisations providing data are kept in a steel closet in the IT department. All data deliveries and deletions are recorded and catalogued. Data storage devices are disposed of with shredding machines and/or by drilling holes in the hard disk.

In general, data are only transferred using password-protected media. When data are transferred, encryption takes place on the data server.

Data are not shared beyond that foreseen in contractual agreements.

## **Data Management Records**

An electronic record is made of all data deliveries and deletions. Record is also made when data are shared in a contractually permissible manner (e.g. with project partners), or when working data sets or partial data sets are created. The modification of the raw data that have been provided to ZEW is not planned or intended.

## **Third-Party Monitoring**

Data are not shared with third parties unless this is foreseen under the governing data usage contract. All project employees who process data are informed of the specific usage conditions that apply. To the extent that third-party service providers are contracted with the processing of personal data within the scope of existing data usage contracts or pursuant to legal regulations that allow for such processing, the agreements signed with these service providers are constructed to ensure that data are processed confidentially and in conformance with the law. Service providers are carefully selected. Furthermore, the agreements that are signed with these service providers address all requirements that must be upheld under data protection laws.

## **Availability Assurance**

ZEW regularly conducts backups of the data sets on its servers. In order to protect against damage or defective hard drives, server data are saved to a second hard drive in real time. All hard drives are located in rooms that have air conditioning, are particularly fireproof, and which are specially marked on emergency action plans. The entire ZEW network is fully documented. Data are backed up to servers located in discrete fire compartments of the building.

## **Data Protection Officer**

The Data Protection Officer has access to all agreements with data suppliers that are relevant to data protection. He provides instructions to project employees concerning data protection requirements and also monitors compliance with contractual agreements by conducting spot checks. The Data Protection Officer must provide approval before employees can be granted access to particularly sensitive data.