Research Data Management Plan - Guidelines for Researchers engaging in Research Subject to the GDPR

Introduction

The EU General Data Protection Regulation (“GDPR”) came into force across the European Union on May 25, 2018, bringing with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. The new Regulation aims to standardize data protection laws and processing across the EU, affording individuals stronger, more consistent rights to access and control their personal information.

This document is designed to act as a reference to ensure that all areas of information security and privacy used for and in the University are secured in accordance to University of Haifa (hereinafter referred to as the “University”) Best Practices.

Purpose

This document provides guidelines for University researches on implementing the data protection rules under the University’s Data Policy and Usage Agreements.

Pursuant to the University policy on information security and privacy, the University is responsible for maintaining the confidentiality, integrity, availability and privacy of the data with which it is entrusted by the researchers and/or scientists

Does the GDPR apply to your research?

The GDPR relates to any research that uses personal data or information which identifies, or may identify an individual or may be used to create a profile regarding an individual, who is alive, and within the European Union ("Personal Data"), meaning the research activity is aimed at residents or civilians which are geographically within the European Union. Consequently, if the research you are conducting does not contain any Personal Data then the GDPR will not apply to your research data or outputs. However, if you do hold any Personal Data on individuals within the European Union (as defined above) as part of your research then this will need to be assessed for GDPR compliance.

The GDPR does not apply to anonymized data, which does not relate to specific individuals.

Compliance with the GDPR and other applicable data protection laws is an aspect of best practice for research in the collection and governance of information.

The GDPR will apply in any circumstance in which there is either a contractual obligation between the University and the organization that provided the data or where the research is designed and aimed to collect Personal Data as defined above.

What do you need to do?

As a University of Haifa Researcher, if the GDPR is applicable to your research, you are responsible for ensuring that your research project is managed in compliance with the GDPR, and to notify the University's Research Authority that the GDPR is applicable to your research so it may oversee and verify and help coordinate with the University's Data Protection Officer, should the need arise.

Consequently, you are responsible to take the following steps:

- ✓ You will be responsible for drawing up a data management plan (DMP). This is an organic document that will help to encourage you to think about what will be done with data and to document how you will manage your data throughout the research activity. Your DMP should include GDPR considerations (See Section 1).

- ✓ You should ensure that a Data Privacy Impact Assessment is conducted for your research, if applicable (See Section 4).

- ✓ You will need to be sure to identify your legal basis for collecting and processing personal data. Pay particular consideration to any special category of data (previously referred to as “sensitive personal information”) that you process (See Section 2).

- ✓ You will need to be sure to maintain documentation on your data processing. This will include identifying your reason for collecting data and any locations/systems that you are using to store or process data (See Section 3).

- ✓ You should be sure to only collect data that is necessary to undertake your research. If you do not need the data, then do not collect it.

- ✓ You will need to ensure that you have appropriate security in place, by coordinating with the University's Data Protection Officer, such as encryption, for the Personal Data that you are holding (See Section 5).

- ✓ You will need to ensure that, if Personal Data is not specifically required for the research and/or its outputs that you anonymize any Personal Data that has been collected as soon as possible after the collection, and that any identifiable information is deleted.

- ✓ You will need to ensure that research data can be archived, preserved and made available for future use. This should involve ascertaining that appropriate consent considerations have been addressed (See Section 8).

- You will be responsible for arranging appropriate data sharing agreements or contractual terms as part of your research. These should include clear descriptions of how the data will be used, stored, shared, archived, etc. (See Section 5).
- You will be responsible for ensuring that any data that is transferred to other parties is done so in a secure manner. At the same time, it is preferable to transfer only statistical or anonymous data, insofar as possible (See Section 7).
- You will need to ensure that data breaches are reported to the University authorities as soon as you become aware of them (See Section 6).
- You will need to sign commitments and other documents defining the activities conducted by researchers and/or scientists (See Appendix B)

Drawing up a Data Management Plan

Data Management Plans (sometimes known as data sharing plans) are useful resources to record how you will be managing and organizing your research data outputs throughout the research process or activity.

Understanding legal basis

If you are collecting and holding personal data, you need to ensure you are holding it under the appropriate legal basis.

For the vast majority of research undertaken at the University, the appropriate legal basis for processing personal data will be Article 6(1)(e), i.e. the “public task” basis.

If you are holding special category data (previously referred to as “sensitive personal” information) such as race/ethnicity, physical or mental health, sexual orientation, etc. you will then need to need to obtain explicit, written consent from the data subjects to permit additional processing of the data, i.e. future research based on the original "special categories of data".

Identifying what personal information you hold

The University is required to maintain documentation on its data processing activities (the reasons for collecting and holding personal data) and the associated assets (the locations or systems holding that data). If the research you are managing contains personal data you will need to inform the University Data Protection Officer (DPO) of its existence.

Once you have identified your data processing activities and associated assets you can then begin documenting additional factors such as your legal basis for processing the data, whether the information is shared with third parties, etc.

Data Protection Impact Assessments

If you are collecting personal data, you should carry out a Data Protection Impact Assessment (DPIA) if that processing is likely to result in a high risk to the rights and freedoms of natural persons.

To complete a DPIA please refer to Appendix A for the appropriate form.

Storing data securely

You must ensure that any personal data you are collecting and/or using as part of your research is stored securely. This may involve ensuring that your storage devices, such as laptops and memory sticks, are appropriately encrypted. You should also ensure that any paper files that you hold and which contain personal data are stored securely in locked filing cabinets or offices.

If you are storing your data in a specific piece of software, you should ensure that this software has appropriate security measures in place. These will often be included as part of the IT procurement process, but if you need further information please contact the University DPO.

If you are intending to store your data on a Cloud-based storage service provider, you should consult with the University's DPO in order to insure you are using a certified provider which adheres to GDPR principles, and receive guidance on how to further manage your cloud-based storage according to data protection principles.

You should ensure that any data sharing which is likely to occur as part of your research project is reflected in your research contract. This will include checking that appropriate clauses on data protection and how data will be managed and shared accurately reflect your research activities.

Minimizing Data Security Threats

Minimizing the research team’s contact with sensitive, individually identifiable data or handling only the minimum amount of sensitive data strictly needed for the research study can substantially mitigate the potential harm caused by a data breach and reduce the required data security measures that need to be put in place. This will often simplify and accelerate the research data flow.

De-Identifying Data

Separate Personal Data from all other forms of data as soon as possible. Data stored by you poses the most risk from a data protection perspective when sensitive or confidential information is linked directly to identifiable individuals.

Once separated, if the “identifier” data set is required for the current or future research and cannot be purged/removed, then it and the “analysis” data set should be stored separately, analyzed separately, and transmitted separately. Once separated, the identifiers should also remain encrypted at all times, and the two data sets should only meet again if necessary, to adjust the data matching technique.

Paper-based surveys should also be designed to enable Personal Data to be removed. All direct identifiers and contact information should appear on a separate cover sheet. To conserve the ability to re-identify the analysis data set, a unique “Study ID” can be created by the researcher and added to both data sets.

One method for creating Study IDs is:

- ✓ Create a random number from a physical source (e.g., dice) or from a pseudo-random number generator.
- ✓ Use the first random number as a “seed,” and use a pseudo-random number generator to sort the observations.
- ✓ Use another random number as a second “seed,” and use a pseudo-random number generator to create a Study ID.
- ✓ Ensure each Study ID is unique.
- ✓ Depending on how the Study ID is created, it may be essential to maintain a secure gateway (i.e., mapping/decoding) between the Study ID and Personal Data. This gateway should be secured both to ensure confidentiality and to prevent data loss.

Encryption

Researchers should consult with the University's DPO in order to ensure that Data be stored and transferred in encrypted form throughout its life cycle using at least one of the following methods.

Device-Level (Whole-Disk) Encryption:

- ✓ Desktop\Laptop – The disk can be encrypted using a hardware utility (bios) or data protection feature that integrates with the most popular operating system (BitLocker in MS Windows, etc.).
- ✓ Flash Drive (Disk on Key) – Recommended to encrypt using a data protection feature that integrates with the operating system. Using hardware-based encryption will prevent access to the Data from an alternate computer if the original computer is lost, for example.

- ✓ Tablets / Mobile phones - For tablets used as primary data collection devices, an application such as AppLock should be used to prevent users from accessing other applications during data collection. This protects data from being transferred across applications. The research team should also enable remote wiping capabilities on these devices in case of loss or theft. After installation and implementation, whole disk encryption should not materially affect the user experience.

Folder-Level Encryption: While cloud storage tools encrypt the connection and files "at rest" on their systems, they retain the encryption keys, which technically gives their employees access to all files saved on their servers. To address this, for highly sensitive data, it is recommended to use tools like Boxcryptor that encrypt files before they are stored in the cloud.

File-Level Encryption: While whole-disk and device-level encryption encrypt all files on a device, they do not protect files once they leave the device, e.g., while they are in transit or being shared with another researcher. File-level encryption applies to specific files and facilitates data sharing. Proper use of file-level encryption requires strong alternative protocols for password sharing for unlocking and relocking files before and after use. Options for file-level encryption include PGP-Zip and 7-zip.

IT-Administrated Options: For researchers operating applications or systems used for sensitive data collection and who have access to a professional IT team, IT-administered options may be preferable. These options allow researchers to delegate the administration of a data access and storage solution to IT experts. IT administrators may also be able to provide several additional levels of data protection. As with cloud storage, IT staff may have access to all data on a server, including Personal Data. Researchers should therefore be sure to understand who has access to the data and maintain as much direct control as possible to prevent compliance issues or accidental data breaches.

Data Storage & Access:

Researchers have many options for secure data storage and access. Relevant considerations for choosing among these options include: the sensitivity of the data, applicable compliance requirements or contractual obligations relevant to that data, the research team's technical expertise, internet connectivity, and access to IT expertise and support.

Institutions may offer space on a server or provide a location to host a server. Storing data on such a server may be preferable to relying on laptops, desktops or cloud storage to retain data.

Access to these servers is typically automatic when connected from a predefined endpoint over internal LAN. Off-site access requires the use of a Virtual Private Network (VPN). This provide additional layers of security by encrypting all network connection and requiring at least one more type of authentication.

Additional security features that may be available upon request include:

- Inactivity timeouts for remote access and endpoint location.
- Non-retrievable passwords: If a user forgets his or her password, the password is reset by the system, rather than the original password being returned.
- Password expiration settings that require a new password to be created on a regular basis.
- Restriction on the number of password guesses permitted before account lockout.
- Access logs that describe who signed in, from where, and when.

IT or data managers may be able to grant access permissions to specific users for specific files or folders on the server. This level of control would enable teams to share general access to a folder while limiting access to identified data to specific members of the team.

Data Transmission and Sharing:

Data must be protected both when at rest and in transit between the data provider, research team members, and partners. Data that are encrypted while at rest on a whole-disk encrypted laptop, or on a secure server, will not necessarily be protected while being transmitted. The options presented below may vary in their level of security.

Unsafe transmission methods include:

- Email without encryption
- Uploading data to nu-managed or nu-approval by the university (e.g. Google Drive owned by someuser@gmail.com will not be secure; however, the same operation to Drive owned by someuser@somedomain.haifa.ac.il will be fine).
- Mailing unencrypted media devices (e.g., CDs, USB memory sticks, flash drives, and external hard drives)
- Password-protected Excel file

Safer transmission methods include:

- Secure Shell File Transfer Protocol (SFTP), including Secure Shell (SSH)
- Uploading an encrypted file to Dropbox or OneDrive, or to Google Drive

- ✓ Emailing an encrypted file and sharing the password separately and securely via an alternative communication method.
- ✓ Mailing encrypted files loaded onto encrypted devices
- ✓ Survey software with encryption features and which supports encryption during data collection and transmission to a central server.

Communication and Data Sharing with Partners:

Many research partners, such as service providers, survey enumerators, and holders of administrative data, have had minimal prior exposure to data security or data sharing protocols. It is best practice to develop a data sharing and security protocol with these partners and to guide them in understanding their role in data security.

All partners handling or transmitting data should be informed of and trained in the data collection, storage, and transfer policies agreed upon for the study, and in the event the Personal Data is subject to GDPA, a Data Protection Addendum/Agreement must be executed in order to regulate and manage the exchange of Personal Data.

Request that partners notify the research team before sharing any data to ensure compliance with the relevant data management plan. Teams should communicate with each other and with partners by referencing Study ID rather than using Personal Data. Consider developing standard operating procedures for:

- ✓ Sharing data and receiving updates
- ✓ Verifying that the data set does not contain unauthorized information prior to downloading, if possible
- ✓ The timeline for reviewing new data for unauthorized information or Personal Data
- ✓ Notifying source breaches and requesting corrective action to prevent future breaches
- ✓ Removal and destruction of files with unauthorized information

Personal Device Security

There are several simple steps researchers and their staff can take to ensure their machines remain secure and to minimize possible weak points, these steps include:

- ✓ Using a password-locked screensaver and timeout lock.
- ✓ Installing and maintaining an approved antivirus and any other security tool recommended by the university's CISO. This software should be kept up to date and allowed to perform regular checks.

- ✓ Making sure the system includes a properly configured firewall recommended by the University's CISO.
- ✓ Removing unnecessary tools and software components installed on the computer.
- ✓ Keeping all OS components and software installed on the system up to date. Most computers and platforms regularly check and notify for new versions of software, so attention should be paid to any notice of update availability and followed up accordingly.
- ✓ Do Not install or run programs from untrusted or not d sources, IT departments generally have recommended software to help secure personal devices and may be able to assist with updating this software or may push automatic updates.

Identification Policies

Strong passwords are essential to ensuring data security. Use Two-Factor Authentication (2FA) for each high-value account. Use different password for each resource, e.g., the passwords for Dropbox, email, institutional servers, and encrypted files should all be different.

In general, strong passwords should:

- ✓ Be at least eight characters long, but preferably much longer
- ✓ NOT contain or solely comprise from:
  - o Dictionary words in any language, even with a varied capitalization scheme or with numbers or symbols substituted for letters (e.g., 1 for l, @ for a, 0 for O)
  - o The name of the department or related words
  - o The user’s name, username, email address, phone number, etc. (forwards or backwards)
  - o Repetitive or sequential letters or numbers

Do not forget your password. Strong passwords may be difficult to remember. When using some software, such as BoxCryptor, a forgotten password is completely irretrievable and means the loss of all project data.

Store and share passwords securely. A password-protected Excel file containing a list of passwords is not a secure way to store or share passwords. Passwords should never be shared using the same mechanism as the file transfer, nor should they be shared over the phone.

Preventing Data Loss

In addition to securing against outside threats, preventing data loss is an essential component of data security. Data and gateways between Study IDs and Personal Data should be backed up regularly in at least two separate locations, and passwords must not be forgotten.

Cloud-based storage tools such as OneDrive, Dropbox and Google Drive offer packages to back up data for several months or more and may insure against unintentional erasure of data if it is noticed within the backup time period; these storage tools are not true backup tools as they do not keep deleted files forever. Backing up data to an encrypted external hard drive (stored in a separate location from everyday computers) is an option for low-connectivity environments.

Data Breaches

A data security breach can result in serious consequences for research subjects, the University, and the researcher. Research subjects may suffer unintentional disclosure of sensitive identified information, which may expose them to identity theft, embarrassment, and financial, emotional, or other harm. Both the University and the researcher may suffer reputational damage and may have more difficulty obtaining sensitive data in the future. A breach will likely trigger additional compliance requirements, including reporting the data breach to the Data Protection Authority (DPA), and, in certain circumstances, to each individual (data subject) whose data was compromised. The data provider may require additional security protections or terminate access to the data. In some cases, there may be financial and/or criminal liability to the data provider and/or the research subjects.

Sensitive data are vulnerable to both inadvertent disclosure and targeted attacks. If data security protocols are not adhered to, data may be disclosed.

The GDPR introduces new obligations to report breaches to the DPA within 72 hours.

The University must notify the DPA if a breach could result in a risk to the rights and freedoms of individuals. **Reporting to the DPA will be done only by the DPO.**

The University must also notify the individuals themselves if the breach could result in a high risk to the rights and freedoms of those individuals.

In order to proactively manage breaches, you should be clear about what a data breach is. Therefore, it is important to ensure that you and your team know how to identify and respond to a breach.

If there has been a breach, immediately contact the Cybersecurity Division to report the incident.

Approval

Prior to receiving any personal data of any research project, Researcher will be required to sign **Appendix E** and confirm that he has read and understood this Directive, and that he will store and process personal data in the scope of the contemplated research project according to this Directive.

Appendix A - Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) are a GDPR requirement and a tool that can assist those with data protection obligations in identifying the risks associated with data processing and posed to data subjects. It enables a pre-emptive approach to assessing the risks, applying corrective actions and mitigating controls before a breach occurs.

A1. IDENTIFYING THE NEED FOR A DATA PROTECTION IMPACT ASSESSMENT.

Not all processing activities will require a DPIA. It is therefore essential that checks be carried out and the predefined screening questions used to ascertain which (*if any*) of the high-risk operations intended to be performed will require an impact assessment.

The questions provided in the screening template cover most of the risks that could be classified as high for a data subject. These questions can be used prior to each assessment proposal.

REF	SCREENING QUESTION	YES	NO	N/A	NOTES
1	Does the processing require systematic and/or extensive evaluation *(via automated means*) of personal aspects of an individual or individuals?	✓			
2	Will decisions be based on such evaluations that are likely to produce legal effects concerning the individual(s)?				
3	Is the processing conducted on a large scale and does it involve special categories of data?				
4	Is the processing conducted on a large scale and does it involve data relating to criminal convictions and offences?				
5	Does the processing involve systematic monitoring of a publicly-accessible area on a large scale (i.e. CCTV)?				
6	Will the project involve the collection of new				

	information about individuals?				
7	Will the project compel individuals to provide information about themselves?				
8	Are you using information about individuals for a purpose it is not currently used for, or in a way in which it is not currently used?				
9	Is the information about individuals likely to raise high risk privacy concerns or expectations?				
10	Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information or to a third party without adequate safeguards in place?				
11	Does the processing involve the use of new technology or systems which might be perceived as being privacy intrusive?				
12	Could the processing result in decisions being made or action being taking against individual(s), in ways that could have a significant impact on them?				
13	Will the project require you to contact individuals in ways which they may find intrusive?				
14	Will any of the processing activities make it difficult for the data subject(s) to exercise their rights?				
15	Will the operation involve processing considerable amounts of personal data at regional, national or supranational level,				

	which could affect many data subjects?				
16	Will the processing involve individuals who are considered “vulnerable”?				
17	Does the processing operation involve any significant risk of the personal information being leaked or accessed externally?				

If you answered **NO** to all of the screening questions, it is unlikely that you will need to carry out a DPIA. You should retain a copy of this completed sheet along with your justification for any of your answers in the notes section.

If you answered **YES** to one or more of the screening questions, you should proceed through the DPIA stages and complete the full assessment. When completed, a copy of your finished screening questions, answers and notes should be retained along with the recorded DPIA documents.

A2. INFORMATION AUDIT

INFORMATION AUDIT			
PERSONAL DATA		JUSTIFICATION	PROCESSING ACTIVITY
What data will be collected?		Why does this data need to be collected? Is there anything you can omit as not necessary?	What processing operation(s) will the data be used for?
Name			
Address			
Post code			
DOB			
Age	✓		
Gender	✓		
Email Address	✓		
Home Tel. No.	✓		
Mobile Tel. No.	✓		
NI Number	✓		
ID Number	✓		
Income/Expenses	✓		
Employment Data	✓		
Ethnic Origin	✓		
Religion	✓		

Health Details	✓		
Convictions	✓		
Credit Data	✓		
Other	✓		

ASSESSMENT QUESTIONS		
REF	ASSESSMENT QUESTIONS	RESPONSE
1	What is the legal basis for processing the information?	
2	Who will have access to the information?	
3	Will there be restrictions applied to access?	
4	Does the data need to be transferred to a third party?	
5	Do you have safeguards in place for transferring?	
6	Will you need to obtain consent to process?	
7	How will consent be obtained and the right to withdraw consent be made available?	
8	Will you have control over the data and be able to update/complete it where applicable?	
9	Will you be using data minimization techniques?	
10	Will data be encrypted and/or anonymized?	
11	How will information be destroyed after it is no longer necessary?	
12	How will information be stored?	
13	Will you be able to act on all rights of data subjects (i.e. objections, rectifications,	

	erasure, access, etc.)?	
14	Will you be able to meet the deadline for supplying information?	
15	Does the processing operation require the Supervisory Authority to be notified?	
16	What security measures are in place to protect identifiable information?	
17	Have all employee, agents and third parties involved in the project been trained in the data protection regulations and impact risks?	
18	What consultations are involved in identifying the privacy issues and risks associated with this project?	
19	Will personal data be transferred to a third country or international organization outside Israel or the EU? If yes, what safeguards and Chapter V GDPR measures are in place?	
20	Detail any other factors or information that can assist in this Privacy Impact Assessment.	

DPIA_Assessment_Templates.xlsx

Appendix B - Obligations and Activities of Researchers and/or Scientists

According to the GDPR, you should ensure data integrity and confidentiality and ensure that data are accurate and where necessary kept up to date.

Every reasonable step should be taken to ensure that personal data that are inaccurate are erased or corrected without delay. Also, data which are not used should be removed, unless these data are needed to be able to verify or reproduce research.

You can protect the information in your data files by:

Controlling access to restricted materials by means of encryption. By coding your data, your files will become unreadable to anyone who does not have the correct encryption key. You may code an individual file, but also (part of) a hard disk or USB stick. All personal sensitive data (stored on cloud/third party) should be encrypted or as a minimum pseudo-anonymized.

Recommended tool by the University: BoxCryptor.

Also, you should not send personal or confidential data via email or through File Transfer Protocol (FTP), but rather by transmitting it as encrypted data.

Computer system security

- ✓ The computer you use to consult, process and store your data, must be secured:
- ✓ Use a firewall to protect your data from viruses;
- ✓ Install anti-virus software;
- ✓ Install updates for your operating system and software;
- ✓ Only use secured wireless networks;
- ✓ Use passwords (see Appendix C) and do not share them with anyone. Do not use passwords on your university computer only, but also on your laptop or home computer. If necessary, secure individual files with a password;
- ✓ Do not provide others with your login credentials.
- ✓ Only allow access to the data to authorized people and withdraw access when they leave.

Physical data security

With a number of simple measures, you can ensure the physical security of your research data:

- ✓ Lock your computer even when leaving it for just a moment (Windows key + L);
- ✓ Lock your door where your laptop and/or desktop PC are if you are not in your room;
- ✓ Keep an eye on your laptop;
- ✓ Do not leave unsecured copies of your data lying around;
- ✓ Carry your USB stick or external hard disk in such a way that you cannot lose it and/or lock them in a secured location when not in use;
- ✓ Keep non-digital material which should not be seen by others in a locked cupboard or drawer.

Destroying data in a consistent and reliable manner when needed

Personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Note that deleting files from hard disks only removes the reference to it, not the file itself. Overwrite the files to scramble their contents or use secure erasing software. For USB and CD/DVD, physical destruction works best to erase data.

Non-disclosure: Participating University scientists shall not use or disclose a Limited Data Set other than as permitted or required by the Agreement or as required by law or otherwise authorized by the University.

Reporting: Participating University scientists shall report to the University's Data Privacy Officer, in writing, any use and/or disclosure of a Limited Data Set that is not permitted or required by the Agreement and of which the participating University scientist becomes aware. Such a report must be made as soon as reasonably possible but in no event more than five (5) business days after discovery by the participating University scientist of such unauthorized use or disclosure. This reporting obligation shall include breaches by participating University scientists or by University employees, subcontractors and/or agents. Each such report of a breach will:

- ✓ identify the nature of the non-permitted or violating use or disclosure;
- ✓ identify the Limited Data Set used or disclosed;
- ✓ identify who made the non-permitted or violating use or disclosure;
- ✓ identify who received the non-permitted or violating use or disclosure;

  - ✓ identify what corrective action the participating University scientists took or will take to prevent further non-permitted or violating uses or disclosures;
  - ✓ identify what the participating University scientists did or will do to mitigate any deleterious effect of the non-permitted or violating use or disclosure; and
- ✓ provide such other information as the project may reasonably request.

Appendix C - Password Construction Guidelines

Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly-constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

Statement of Guidelines

Strong passwords are long; the more characters there are, the stronger the password. We recommend a minimum of eight (8) characters in a password. In addition, we highly encourage the use of passphrases, i.e., passwords made up of multiple words. Examples include “It’s time for vacation” or “block-curious-sunny-leaves”. Passphrases are both easy to remember and type yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

- Contain seven or fewer characters.
- Contain personal information such as birth dates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of “Welcome123” “Password123” or “Changeme123”

Strong passwords have the following characteristics:

- Contain both upper- and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

In addition, every work account should have a different, unique password.

Appendix D - CHECKLIST

ASSESSMENT CHECKLIST		
REF	**ASSESSMENT QUESTIONS**	**RESPONSE**
1	Do you separate (Personal Data) from all other data as soon as possible?	
1.1	Is the “identifier” data set stored separately?	
1.2	Are the identifiers stored encrypted?	
2	What method for creating Study IDs do you use? (describe):	
3	Are computers, flash drives, tablets, mobile phones, and any other hardware used for data storage and/or primary data collection whole-disk encrypted?	
4	Do you encrypt files before they are stored in the cloud?	
5	What file-level encryption tool do you use?	
6	Does off-site access use a Virtual Private Network (VPN)?	
	Use of VPN includes:	
6.1	□ Inactivity timeouts for remote access	
6.2	□ Non-retrievable passwords. If a user forgets his or her password, the password is reset by the system, rather than the original password being returned.	
6.3	□ Password expiration settings that require a new password be created on a regular basis.	
6.4	□ Restriction on the number of password guesses permitted before account lockout.	
6.5	□ Access logs that describe who signed in, from where, and when.	

7	Do you transmit the data securely?	
	Transmission methods include:	
7.1	□ Secure Shell File Transfer Protocol (SFTP), including Secure Shell (SSH)	
7.2	□ Uploading an encrypted file to Dropbox or OneDrive, or Google Drive	
7.3	□ Emailing an encrypted file and sharing the password separately and securely	
7.4	□ Mailing encrypted files loaded onto encrypted devices	
7.5	□ Survey software with encryption features, that supports encryption during data collection and transmission to a central server	
8	Do you use a password-locked screensaver and timeout lock?	
9	Do you install and maintain antivirus software?	
10	Do you keep this software up to date and allow it to perform regular checks?	
11	Do you use an operating system with a built-in firewall?	
12	Is all software you use up to date?	
13	Are your passwords at least eight characters long?	
14	Do you back up data to an encrypted external hard drive?	

Appendix E – RESEARCHER APPROVAL

To: The University of Haifa

I declare and confirm the following:

a. I am engaged in the research project ______________________ (“Research Project”).

b. In the scope of such project I am required to store personal data, and I have been advised that such data is subject to European regulation in respect to privacy protection, and that I am required to abide by such regulation.

c. I have read and understood the above Directive, and agree to carry out the Research Project in accordance with the Directive.

Full Name: ______________________

Date:

Signature: ________________