Clusterfy

Standard Data Processing Policy

GDPR Compliant

EFFECTIVE DATE	DECEMBER 26, 2023
POLICY VERSION	V. 1.0
REVISION DATE	DECEMBER 26, 2023

1. Introduction and Recitals

Clusterfy, a forward-thinking technology firm driven by innovation and commitment to excellence, is dedicated to harnessing the of artificial intelligence through our cutting-edge platform, SynapseGPT. At the heart of our services lies the steadfast principle of processing data from client organizations (the "Data Controller"), wherein Clusterfy serves as the entrusted "Data Processor."

The collaborative partnership between the Data Controller and Data Processor, collectively referred to as the "Parties" and individually as a "Party," is grounded in our mutual understanding and dedication to maintain the strict confidentiality and integrity of all processed Personal Data. This alignment is further epitomized through our shared compliance with the General Data Protection Regulation (GDPR) and other relevant data protection laws that safeguard personal data privacy rights.

In our unwavering commitment to honor our in the course of business activities, Clusterfy receives access to personal data controlled by the Data Controller, manifesting a profound responsibility protect and manage data with the utmost care. This document outlines the Data Processing Addendum which is crafted to ensure that the Data Controller can its data protection obligations under GDPR and other applicable data protection legislation.

It states our collective approach to the Commissioned of personal data, as well as terms herein, which strive for the highest of lawful and ethical data processing practices Clusterfy's resolve in protecting Personal Data is reflective of our broader responsibility not to our clients but to the end users – the Subjects. By robust and transparent processing parameters, Clusterfy is not complying with legislation is actively advocating for the respect and protection of individual rights.

These are integral to our mission, reinforcing the trust placed us as we innovative solutions such as SynapseGPT to empower businesses and users alike the ever-evolving digital landscape.

2. Definitions

1. “Personal Data” shall mean any information relating to an or identifiable natural person (a “Data Subject”) that is used or processed by the SynapseGPT platform provided by Clusterfy. This encompasses, but is not limited to, data such as names, contact details,

and any other information that SynapseGPT may come into contact with during its standard operations when engaged by Users or Enterprises.

2. “Data Controller” refers to any User or Enterprise that determines the purposes and means of processing of Personal Data using SynapseGPT.

3. “Data Processor refers to Clusterfy when it processes Personal Data on behalf of the Data in the course of providing SynapseGPT services.

4. “Sub-Processor” means any entity that is engaged by Clusterfy to assist fulfilling its obligations with respect to the provision of SynapseGPT under Addendum and where such entity processes Personal Data.

5. “GD” (General Data Protection Regulation) refers to Regulation (EU) 6/679, a legal framework that sets guidelines for the collection and of personal data within the European Union.

6. “Standard Data Processing Handbook refers to the set of terms, conditions, standards, and guidelines established Clusterfy for the processing of Personal Data through SynapseGPT.

7. “Users” refers to individuals who are authorized to use SynapseGPT platform and can interact with it, whether they are employed by or associated with an Enterprise customer of Clusterfy.

8. “Enterprises” or "Clients" refers to any business entity, organization, or institution that has entered into a service agreement with Clusterfy to utilize SynapseGPT for processing its data.

9. “Data Protection Law” shall include the GDPR, any and all other applicable laws, and secondary legislation in any jurisdiction related to the use and protection of Personal Data, including laws governing the export of data outside the jurisdiction.

10. “Commissioned Processing” shall denote the processing of Personal Data carried out by SynapseGPT pursuant to the documented instructions of the Data Controller and in with the Standard Data Processing Handbook and the service agreement between Clusterfy and Data Controller.

11. “Technical and Organizational Measures” shall mean all measures implemented to ensure a level of security appropriate to the risk, but not limited to measures concerning the security of the SynapseGPT, data encryption, access controls, system audits, and incident response protocols as in further detail in the Standard Data Processing Handbook.

2.1 Personal Data

In the course of state-of-the-art artificial intelligence solutions through SynapseGPT, Clusterfy recognizes the utmost importance of handling Personal Data with the highest standards of privacy and security. The types of Personal Data that may be processed when utilizing SynapseGPT include, but are not limited to:

- User identification data, such as names, job titles, and contact information, which includes work addresses and phone numbers.

- User authentication data, including login credentials for accessing SynapseGPT and associated services.
- Interaction data reflecting the usage patterns, preferences, and commands made by users within the SynapseGPT environment.
- Other relevant information provided the users or generated SynapseGPT as a result of processing requests, which might involve company data and insights.

Clusterfy ensures that processing of Personal Data through SynapseGPT align strictly with the principles and requirements set forth by the General Data Regulation (GDPR). This includes obtaining clear and explicit consent from the subjects, ensuring the accuracy of the data processed, and maintaining integrity and through state-of-the-art technical and organizational measures.

All Personal Data processed through SynapseGPT will only be utilized for the purposes consented to by the data subjects and outlined in the contractual agreements. This ensures that the data subjects maintain control of their Personal Data, and are afforded all rights without exception as stipulated under GDPR such as the right to access, rectification, erasure, restriction processing, data portability, and the right to object.

Clusterfy to transparent and responsible data processing practices, detailed documentation and guidance to and businesses on how SynapseGPT processes and protects Personal Data. We will continually assess and adjust our data handling procedures to align with evolving regulatory requirements and best practices, safeguarding the Personal Data entrusted to us part of our commitment to our users' privacy.

2.2 Data Subject

As Clusterfy, we recognize the criticality of accurately identifying and processing personal data of individuals, known as Data Subjects, in the course of using SynapseGPT. The following types of personal data pertaining to Data Subjects may be processed SynapseGPT:

- Full
- Contact Information including work email addresses and phone numbers
- Organization Affiliation and Job Title
- Location such as city and country
- Professional Background Information
- Interaction and Usage Data specific to SynapseGPT, such as queries inputted and results generated within the platform.

Data Subjects can from employees and representatives of our clients who interact directly with SynapseGPT, to their own customers whose personal data might be fed into Synapse GPT as part of the processing services.

We value our commitment to GDPR its principle of data minimization, ensuring that only data necessary for the processing tasks is by SynapseGPT. Our platform employs advanced pseudonymization and data categorization techniques which ensure that personal data is processed in a manner that permits the identification of Data Subjects only long as is necessary for processing purposes.

We store Personal Data in secure with strict access controls in place, and we log data processing activities to an auditable trail of SynapseGPT's interaction with Data Subjects.

Furthermore, we respect the rights of Data Subjects under GDPR, which the right to access, rectify, erase, and restrict processing of personal data, as well as the right to object to processing and the to data portability. We provide mechanisms through which Data Subjects - whether are end-users within our client organizations or the clients' customers - can these rights, ensuring transparent and responsive communication channels in collaboration with our Data Officer (DPO).

Clusterfy is committed to ongoing compliance with GDPR, including providing clear information to Data Subjects about the processing of their data maintaining data integrity and confidentiality, and implementing robust data security measures.

2.3 Data Processor

As part of Clusterfy's commitment ensuring the highest standards in data processing and compliance with data protection legislation, we, Clusterfy, engage with SynapseGPT as a key tool in our data processing arsenal. Utilized across a breadth of business functions, SynapseGPT aids in delivering solutions that inherently process substantial datasets that may contain personal data as dictated by the tasks it performs for our clients.

SynapseGPT operates strictly within the parameters set forth by the Data Controller, which in most instances is Clusterfy itself, or our clients when they apply SynapseGPT's capabilities to their data. It is programmed to follow the explicit instructions provided by the Data Controller regarding the nature, scope, and of data processing. Our Internal Data Handling Policy and Client Data Processing Agreements govern these directives to ensure compliance with GDPR other relevant data protection regulations.

Additionally, have assigned a designated contact for data protection matters concerning use of SynapseGPT, ensuring accountability and a clear line of communication for any data issues that arise. This contact person is tasked with overseeing compliance with data laws, facilitating audits, responding to data subjects' requests, and liaison with supervisory authorities as required.

We undertake to use SynapseGPT within its technical capabilities to implement adequate safeguards for the personal data it processes. includes employing measures like access control, data pseudonymization and encryption, ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems services.

Our Technical and Organizational Measures, outlined in detail within our Protection Addendum (DPA), provide a robust framework that guides the of SynapseGPT. They are designed to withstand risks associated with processing activities and are subject to regular review and updates to align with technological and evolving data protection laws.

Clusterfy, as the Data Processor when SynapseGPT, ensures all processing of personal data is consistent with GDPR obligations. We monitor SynapseGPT's performance to avoid Noncommissioned Processing Activities and make certain that all personnel involved in data processing are trained GDPR compliance and bound by confidentiality agreements.

In the context of GDPR and our role as a Data Processor, we Clusterfy pledge unwavering adherence to the compliance framework, guaranteeing our clients' utilization of SynapseGPT is both effective as it compliant with the highest data protection standards.

2.4 Data Controller

In the capacity of Clusterfy, we act as the Data Controller in relation to the personal data processed part of our services provided through SynapseGPT. As the Data Controller, we determine the purposes and means of processing personal data of our clients and their end-users.

We recognize and uphold our responsibilities under GDPR to ensure that all personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subjects. We are committed to implementing appropriate data protection policies, IT and security measures ensure we meet the GDPR and safeguard the personal data entrusted to by our clients.

We maintain comprehensive records of data processing activities and ensure that all processing is conducted in accordance with our Data Protection Policy, as outlined our Standard Data Processing Handbook. We ensure that consent from data subjects is wherever necessary, and that the legitimate interests for certain processing activities are properly and articulated.

Furthermore, as Data Controller, we are dedicated to data subjects' rights, including the right to access, rectification erasure, of processing, data portability, and the right to object. We have established protocols to respond to data subjects' requests in a timely manner, compliance with GDPR requirements.

In the event data needs to be transferred to third or across borders, we take the necessary precautions to ensure data protection, including execution of Data

Processing Agreements (DP) with all our processors, subordinates, and partners. All such data transfers are in compliance with our Data Processing Terms, ensuring the security and confidentiality the personal data through entire processing lifecycle.

Our dedicated Data Protection Officer (DPO) (contact details are readily available), oversees all data processing and ensures continuous with the GDPR. Our DPO also acts as point of contact supervisory authorities and data subjects in matters relating to data protection.

As Clusterfy and Data Controller, we take our duty to protect data seriously and are committed to upholding the principles of GDPR in every of our processing activities through SynapseGPT and any other data processing operations. We ensure that personal data is processed for specified, explicit, and legitimate and not further processed in a manner incompatible with those purposes.

2.5 Others (Additional definitions as necessary)

As Clusterfy, we further elucidate the following definitions to complement and provide clarity within the overarching context of our Data Processing Terms as they relate to SynapseGPT and its application within business operations:

2.5.1 “SynapseGPT” refers the proprietary artificial intelligence platform developed by Clusterfy, designed to perform various tasks including but limited to document analysis, summary generation, automated text generation based on specified instructions, and integration with multiple systems and tools using technologies such as natural language processing and machine learning.

2.5.2 “User” shall mean any individual or entity that interacts with or utilizes SynapseGPT, whether they employees of Clusterfy, clients, contractors, or any end users authorized Clusterfy.

2.5.3 “Clusterfy Technologies” aims to the unique assemblage of methodologies, software, algorithms, tools that are part of the offerings of Clusterfy, including SynapseGPT functionality and related services.

2.5.4 “Personal Configurations” refers to the specific settings, preferences, rules and protocols set up within SynapseGPT by the User to adapt platform to particular processes, workflows, or tasks required by Clusterfy or clients.

2.5.5 “Data Subject Interaction shall mean any interaction between a data subject (as defined in the General Protection Regulation) and SynapseGPT, including data entry, queries and data processing activities.

2.5.6 “Automated-Making” as it pertains to SynapseGPT, shall refer the ability of the platform to make decisions without human intervention, based on-established criteria, algorithms, or rules implemented by the User within the Personal Configurations of SynapseGPT.

2.5.7 Integration Interface” shall refer to the specific components, APIs, and connectors SynapseGPT allow for seamless communication and data exchange with third-party systems, tools, and applications.

2.5.8 “Operational Efficiency Metrics” shall mean the metrics and measures used to evaluate the improvement in performance, productivity gains, error reduction, and speed enhancements attributed to the implementation of SynapseGPT business processes.

Each of these definitions lays the foundation to ensure clear understanding and compliance with our Data Processing Terms while adopting SynapseGPT for innovation and automation.

3. Details of the Commissioned Processing

1. Subject Duration of the Services to be Carried Out

The subject and duration of the work to be carried out are set forth in the Services Agreement between Clusterfy and the Data Controller. Clusterfy, as the Data Processor, commits to processing personal data for the duration the Services Agreement, solely for the purposes of providing the functionalities of SynapseGPT as stipulated in our Agreement of Personal Data.

The following types of Personal Data and/or Personal Data shall be the subject of the Commissioned Processing:

- User information including not limited to names, contact details, and job titles; Usage data from SynapseGPT including log-in credentials and interaction timestamps;
- Content data supplied by the users in the course of using SynapseGPT, such as text inputs for processing and generated outputs- Any other data that Processor accesses as a result of performing the Services in the Services Agreement.

3. Purpose of the Commissioned Processing

Clusterfy shall process Personal Data solely as necessary to deliver the services of SynapseGPT per the Services Agreement to the Data Controller. This includes but is limited to natural language processing tasks, data analysis, and summaries, as text generation according to the specific requirements of the Data Controller.

4. Type and Extent of the Commissioned Processing

The extent of processing carried out by Cluster includes the collection, retrieval, and analysis of Personal Data provided by the Data Controller. All processing activities by Cluster shall be conducted in accordance with the terms outlined in the Services Agreement, and only upon instructions provided by the Data Controller.

5. Categories of Data Subjects

Clusterfy will process Personal Data regarding the following categories of data subjects as for providing the SynapseGPT:

- Employees of the Data availing of the SynapseGPT services;
- Clients of the Data Controller and their respective personnel whose data may be processed through the use of SynapseGPT for business functions as agreed upon in the Services Agreement.

6. Technical and Organizational Measures

Clusterfy will implement, maintain, update the 'Technical and Organizational Measures' as detailed in Annex 1 to the Data Processing Addendum. Those measures are to secure the Data against accidental or unlawful destruction or loss, disclosure, unauthorized access, and other unlawful forms of processing.

7. Rectification, Erasure, and Related Obligations

Clusterfy will promptly relay such requests to the Data within three (3) business days. Handling of these requests, including any data portability or to processing, will be the responsibility of the Data Controller.

Clusterfy understands the sensitive nature of the Personal Data processed and the requirements come with handling such data under the GDPR and the Standard Data Processing Terms outlined in the Data Processing Addendum.

3.1. Subject Matter and Duration of the Services

In accordance with the provisions of our Standard Data Processing Handbook, the subject matter of the services that Clusterfy will provide shall encompass the implementation, operation, and maintenance of the SynapseGPT platform. This platform is designed to enhance business processes and decision-making through advanced artificial intelligence capabilities including but not limited to natural language processing, machine learning models, and automation technologies.

The services provided will be tailored to meet the specific requirements of our clients, in the setup, customization, and integration of SynapseGPT into existing systems and workflows. Engagements may include data analysis, document summarization, automated text generation and the seamless of the platform to support various business functions such as human resources, sales, project management, finance, and compliance.

This will be effective upon the signing date and will remain in effect for a period of [insert duration in years, months, or as specified by project scope or contract]. This duration reflects our commitment to provide sustained support, routine updates, and the necessary modifications to the SynapseGPT platform to ensure its relevance effectiveness in supporting our clients' evolving needs. Upon the conclusion of this period, the contract may be to renewal following a review of services, and mutual agreement between Clusterfy and the client.

3.2. Types of Personal Data

In the course of providing our services through the SynapseGPT platform, we may process the following types of Personal Data, which are necessary to deliver the bespoke functionalities intelligent solutions our clients require:

- Organization-related data:
    - Legal Entity Name: The full official name of the client’s organization.
    - Business Registration Details: Registration number or identifier that is unique to each client's entity.
    - Sector-Specific Information: Data relevant to the specific industry sector in which client operates.
- Contact Information:
    - Business Address: The physical and/or mailing address for client’s organization.
    - Contact Details: Email addresses and phone numbers for points of contact within the client's organization, including title and department as necessary for our and provision of services.
- User Account:
    - Account Identifiers: usernames, user ID numbers or account numbers to individual users.
    - User: Information such as job titles, roles, and all associations to user experiences and access within SynapseGPT

- Technical Data - Log Data: Information automatically collected by our, such as addresses, device identifiers, browser types, and operating system details are necessary for diagnosing technical issues and ensuring the security and operation of SynapseGPT.

- Data Generated from Use of SynapseGPT:
  - Interaction Data: Logs and records of user interactions with the system, used to improve system performance and user experience.

- Financial Information and Billing Information: Data necessary to process payments for services provided, such billing address and tax/VAT ID, subject to additional security measures and as required for transactional purposes.

- Organizational Behavioral Data:
  - Patterns: Anonymized or aggregated data reflecting the ways in which clients SynapseGPT features, helping to enhance system intelligence and predictive capabilities. Clusterfy, through SynapseGPT, is committed to processing these of Personal Data in accordance with the highest standards of privacy and security, as mandated by the General Data Protection Regulation (PR) and other applicable data protection laws.

3.3. Categories of Data Subjects

As part of our commitment to uphold the integrity and confidentiality of personal data processed through SynapseGPT, we recognize the necessity clearly identify the categories of data subjects involved. In accordance with the Standard Data Processing Handbook, Clusterfy processes personal information relating to the following categories of data subjects:

a) Employees of Clusterfy: Personal data of our employees are processed for purposes consistent with human resources management, including but not limited recruitment, payroll, training, and other administrative functions necessary for the operation of our business.
b) Clients/Customer Contacts: We process personal details such as contact information of individuals representing organizations. This data facilitates communication, contract management, service delivery, and ongoing business relationships.
c) Users of SynapseGPT: Data here include individuals from client organizations and other entities who directly interact with SynapseGPT platform. Processing user data enables us to customize user experiences provide technical support, and ensure secure access to our services.
d) Candidates for Employment: In efforts to attract and recruit top talent, we personal data of job applicants. This includes contact information, qualifications, and pertinent information provided during the application process.
e) Suppliers and Partners: Contact information and other relevant details of our suppliers and business partners processed to ensure efficient supply chain management, procurement, and collaborative endeavors.

data processing activities for these categories are guided by a commitment to protect and respect privacy rights, all within the framework established by GDPR and other relevant data regulations. Clusterfy ensures that all personal data is handled with utmost care and security, limiting access only to authorized personnel who require such to perform their job functions effectively.

3.4. Technical and Organizational Measures

At Clusterfy, we prioritize the security and integrity of the data processed through our SynapseGPT platform. Recognizing the importance of safeguarding personal data in compliance with the General Data Protection Regulation (GDPR), we have implemented a robust of technical and organizational measures designed to protect data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures are consistent with the industry standards and appropriate to the risks presented by our data processing.

Our measures include, but are not limited to:

1. Encryption: All personal data processed through SynapseGPT is encrypted in transit and at rest using strong encryption protocols. This that data is protected against unauthorized access and remains confidential.

2. Access Control: We enforce stringent access control to our systems and data processing. Only authorized personnel with a legitimate need to access personal data for the of their job responsibilities are granted access. We employ multi-factor authentication and review of access rights to prevent unauthorized access.

3. Data Segregation Personal data is logically from other data sets within our system. This ensures that data collected for purposes is processed separately, reducing the likelihood of unauthorized or accidental use.

4. System Integrity and Resilience: Our systems are designed to ensure integrity, availability, and resilience. Regular backups and a robust disaster recovery are in place to allow restoration of data and system availability in the event physical or technical incidents.

5. Regular Testing and Evaluation: We perform testing and security assessments to evaluate and improve the effectiveness of our technical and measures. This includes periodic penetration testing and security audits by independent third- party.

Our organizational measures include, but are not limited to:

1. Protection Policies: Clusterfy maintains up-to-date data protection policies and procedures that are communicated to all employees. These policies are aligned with GDPR requirements reflect our commitment to data protection.

2. Training and Awareness: We regular training to our employees on data protection and privacy matters. This ensures all personnel handling personal data are aware of their obligations and the importance of data subjects' rights.

3. Data Processing Agreements: When engaging third-party service providers or sub processors, Clusterfy ensures that their under GDPR are contractually bound and adhered to. We require allors to implement adequate technical and organizational measures and to submit their data processing for regular audits.

4. Incident Response Plan: In case of a data breach or security incident, Clusterfy has a formalized incident response plan that includes notifying the appropriate supervisory authority and affected data subjects in compliance with GDPR timelines and requirements.

Clusterfy is dedicated to maintaining the highest of data protection continuously monitors and updates its policies and measures to adhere to new regulatory requirements and security best practices.

4. Control of Instructions

As Clusterfy, we understand the importance of adhering to strict instructions regarding the processing of Personal Data to maintain compliance with the GDPR. To this end, we employ stringent control protocols to ensure that all Personal Data processed through our SynapseGPT platform is handled in exact accordance with the instructions provided by our clients, who act as Data Controllers.

In keeping with our commitment to comply with documented instructions from our Data Controllers, we undertake the following responsibilities:

1. Clusterfy will process Personal Data exclusively within the scope of the tasks outlined in the contractual agreement, ensuring that our actions as a Data Processor strictly align with Data Controller directives.
2. We will not any Personal Data for purposes that exceed the instructions provided by the Data Controller or engage in Non-Commissioned Processing Activities. Any change in processing scope must receive direct approval from the Data Controller.
3. Upon receiving a new processing instruction from a Data Controller, Clusterfy conduct a thorough review to confirm it aligns with the GDPR and our policies. If we encounter any instructions, we believe may contravene Data Legislation, we will immediately consult with the Data Controller to seek clarification and will refrain from processing until the instruction is confirmed or suit modified.
4. Clusterfy has established procedures for documenting the processing instructions received, which are stored securely and treated with the utmost confidentiality.
5. We will maintain transparency our Data Controllers by providing them, upon request, with records of processing activities that demonstrate compliance with their instructions and the requirements the GDPR.
6. Any updates, alterations, or new instructions from the Data Controllers will be communicated to all relevant personnel within Clusterfy to prevent unauthorized or incorrect processing Personal Data.
7. In the event of a Data Subject's request for access, rectification, erasure, or data portability, Cluster will promptly relay this request to the Data Controller and await further instruction,aining from unilateral action unless expressly authorized to do so.

5. Control of Data Entry

To ensure the ability to verify and determine whether personal data has been entered, modified, or deleted in the data processing systems, and if so, by whom, Clusterfy will implement data entry control measures in accordance with its Standard Data Handbook. This includes the implementation of mechanisms to ensure the accuracy and quality of the data entered in relation to the use of SynapseGPT by our users and businesses.

Each data entry process in SynapseGPT will be logged to provide a complete audit trail that captures who entered or modified data, when, and what specific changes were made. Additionally, robust credential-based authentication will be required for employee access to the system, with clearly defined authorization levels, ensuring that only employees with the necessary authorization can access or modify sensitive data.

Furthermore, SynapseGPT will be configured to automatically alert designated managers when a significant data modification occurs, providing the ability to review and validate such changes to maintain data integrity. These alerts will also be used to monitor any unusual activity that may indicate a system breach and respond promptly to such scenarios.

Policies and procedures will be regularly reviewed and updated to reflect the latest best practices and technologies to continually enhance the reliability and security of the data entry process. Clusterfy will provide regular training to all employees regarding their responsibilities and procedures for data entry and manipulation to ensure consistent implementation of these control measures.

6. Control of Availability

Clusterfy, operating under strict adherence to the General Data Protection (GDPR), has implemented comprehensive technical and organizational measures to ensure the control of availability and resilience of the systems and services utilized for SynapseGPT.

"Availability control" refers to the that guard against accidental or unlawful destruction or loss of personal data. In order to carry out these protective measures, we employ a multi-layer approach that encapsulates both physical and digital contingencies.

Firstly, data within the SynapseGPT platform is regularly backed up to mitigate the of loss due to any unforeseen circumstances. These backups occur across multiple geographically distributed and secure locations to ensure that personal data can be restored in timely manner if necessary.

Furthermore, Clusterfy maintains a robust disaster recovery which is tested regularly to confirm our ability to promptly reinstate system availability the accessibility of personal data following a physical or technical incident. Our infrastructure designed to be resilient and fault-tolerant, with redundancy built into components. In the event of a system failure, failover mechanisms are to switch operations to standby systems with minimal service interruption.

To ensure operational continuity, Clusterfy employs state-of-the-art monitoring tools to supervise system in real-time. Alarms and notifications are configured to promptly alert the team of any issues that might impact the availability of personal data. The to such incidents is guided by a clearly defined Incident Management Policy, ensuring action and resolution.

Our commitment to data protection and cybersecurity extends to regular training for our personnel, who are well-equipped to apply best practices for ensuring data. This includes the proper handling of incident responses and an understanding of their respective roles within our overall data management strategy.

Clusterfy assures the Controllers that we will rectify, erase, and personal data strictly following their instructions. All measures are in place to meet standards set forth by GDPR, assuring the Controllers that Clusterfy has vested interest in maintaining the highest level of availability controls for personal data processed SynapseGPT.

7. Control of Data Separation

In line with Clusterfy's commitment to ensuring the privacy and confidentiality of the personal data under our management, we have established rigorous controls to uphold data separation. Each's data is treated with the highest level of care and is processed in an environment that logically isolates their personal data from that of other clients.

Our SynapseGPT platform incorporates advanced technological measures to segregate datasets per each of our valued clients. This is achieved by employing a combination of unique client identifiers, role access controls, and strict authentication protocols. We employ secure multi-tenancy architecture ensuring that each client's data environment is distinct invisible to other tenants.

Each user account within our platform assigned distinct permissions that limit access to data based solely on user roles and specific needs of their position. This ensures that team members only access the necessary for their direct tasks, enhancing our compartmentalization efforts. Audit trails are meticulously maintained, capturing all activity around data access and actions taken within the extent of our operations.

We strictly adhere to the GDPR principle of 'purpose limitation,' where processing is limited strictly to the purpose agreed upon with our clients and consent to by the data subjects. All functionalities of SynapseGPT are designed to respect these confines, barring any processing, copying or alteration of beyond the explicit instructions furnished by our clients the data controllers.

Additionally, we have implemented policies and procedures that ensure all data collected for different purposes are processed. This encompasses the separation of data at stage, including collection, processing, and communication.

Clusterfy remains at forefront of safeguarding data integrity and privacy which is pivotal for the unwavering trust our clients place in us. Our data separation protocol a testament to relentless pursuit of excellence data protection and GDPR compliance.

8. Data Processor Obligations

Clusterfy, as the Data Processor, acknowledges and commits to fulfilling responsibilities with respect to the processing Personal Data received from or on behalf of Data Controllers, in line with the GDPR requirements, and following our outlined in the Standard Data Processing Handbook.

In recognition of our role, we shall:

1. Process Personal Data exclusively for the purposes of providing our services under our agreement with the Data Controller, strictly accordance with their documented instructions, unless required by law to act without such instructions. Such legal requirements shall be communicated to the Data Controller prohibited by criminal law.

2. Ensure that all persons to process the Personal Data have committed themselves to confidentiality or are under an statutory obligation of confidentiality.

3. Implement and maintain appropriate technical and organizational as specified in our Standard Data Processing Handbook, designed to ensure a level security appropriate to the risks of our data processing activities, protecting against unauthorized illegal processing and against accidental loss, destruction, or damage.

4. The conditions for engaging another processor (sub-processor), maintaining control over data processing activities subcontracted to them, in correspondence with the policies outlined the Handbook, ensuring sub-processors meet the same data protection obligations as set out in our agreement with the Data Controller.

5. Assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, the fulfillment of the Data Controller’s obligation to respond to requests for exercising data subject's rights under the GDPR.

6. Assist the Data Controller ensuring compliance with their data protection obligations with regard to the security of Personal, the notification of data breaches, and data protection impact assessments, considering nature of processing and the information available to Clusterfy.

7. At the choice of the Data Controller, delete or return all Personal Data after the of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data.

8. A record of all categories of processing activities carried out on behalf of the Controller, containing the information required by the GDPR, and allow for audits including inspections, by the Data Controller or another auditor mandated by the Data Controller, adhering to the Standard Data Processing Terms.

9. Promptly the Data Controller if, in Clusterfy’s opinion, an instruction given the Data Controller infringes the GDPR or other Union or Member State data provisions.

Clusterfy understands the trust our clients place in us and commits upholding their data security interests and compliance obligations under the GDPR, thereby that the use of our platform, SynapseGPT, by users and companies, satisfies all necessary regulatory requirements as stipulated within the Standard Data Processing.

8.1. Usage of Personal Data

At Clusterfy, we acknowledge the paramount importance of protecting personal data and strictly adhere to the guidelines established by the General Data Protection Regulation (GDPR). commitment is to process personal data solely for the explicit and legitimate purposes communicated to our data subjects at the point of data collection through subsequent notifications.

When engaging with our SynapseGPT platform, we ensure that the processing operations align with the intentions articulated by our users and abide by stringent security protocols. These operations may consist of carrying out user-instructed natural language processing tasks, data analysis, document processing, and other AI-powered services that facilitate efficiency and decision-making.

We handle personal data with the utmost care, employing it exclusively for enhancing user experience and platform functionality. includes personalization services, troubleshooting, technical support, and informing about updates or new features Consistently, data subjects are duly informed about the scope of data and given full autonomy over their personal data.

Furthermore, we distinctly acknowledge responsibility in preventing unauthorized access and misuse of data. Clusterfy implements industry-standard technical and organizational measures to safeguard data any breach of security.

As continue to evolve and innovate, our of personal data will reflect advancements in our – always congruent with our ethical and regulatory requirements. Any changes to our usage purposes will be communicated transparently our data subjects, ensuring ongoing compliance and alignment with GDPR principles.

8.2. Support to the Data Controller

In recognizing the significant responsibilities that fall upon the Data Controller under the GDPR framework, Clusterfy commits to providing full assistance ensure that you are able to comply with your data protection obligations.

Our assistance will extend to the handling of any requests from Data Subjects concerning their Personal Data processed by SynapseGPT. We will implement effective mechanisms to enable you, as Data Controller, to respond to Data Subjects' requests for access, rectification, assure data portability, or to the processing of their Personal Data, within the legal time frames. Furthermore, in the instance of a Personal Data breach, Clusterfy promises to notify you without undue delay after becoming aware of it. We understand the urgency gravity of such breaches and are fully prepared to cooperate with you in the, mitigation, and reporting to the relevant supervisory authority as well as to impacted Data Subjects as necessary.

To transparency and accountability, Cluster will maintain clear records of data processing activities, which will be made available you upon request. Our records will illustrate compliance with our obligations under the, as well as serve as a resource for you to demonstrate your organization compliance.

Considering the likelihood for audits by supervisory authorities, Clusterfy also support you with any data protection impact assessments related to SynapseGPT, and where required, will contribute to ensuring that consultations with supervisory are handled effectively and efficiently.

We guarantee that all personal data transferred to will be subject to adequate technical and organizational measures, ensuring a level of appropriate to the risk as highlighted in the GDPR. In fulfilling the role Data Processor, we will only act on documented instructions from you, the Data Controller.

Clusterfy is dedicated to a collaborative approach, understanding that being proactive transparent is key to managing and safeguarding the rights of Data Subjects. team will be at your disposal to provide assistance and to offer any necessary or action to support your role as Data Controller, ensuring that our use SynapseGPT meets the stringent requirements of GDPR.

8.3. Erasure of Personal Data

Upon the conclusion of the data processing services, Clusterfy, acting as the Data Processor, shall, at the choice of Data Controller, return all the Personal Data transferred including all existing copies thereof to the Data or delete all the Personal Data in a secure manner according to data erasure best practices and certify to the Data Controller that it has done so, unless any legal requirement imposed upon Cluster prevents it from returning or destroying all or part of the Personal Data transferred.

Clusterfy's approach to data erasure is to align with the GDPR principle of Right to Erasure (also known 'Right to be Forgotten'). Upon receiving a valid data erasure request the Data Controller or an individual data subject, Clusterfy will promptly initiate process of deleting the relevant Personal Data from all active systems and backups in secure manner. This includes ensuring that Personal Data is irretrievable from SynapseGPT systems.

In the event of data erasure, Clusterfy will keep a log of the erasure requests and confirmations of erasure which can be provided to the Data for audit purposes, subject to the confidentiality agreements in place. This log records the details of the erasure request, including the date and time the request, the data subjects concerned, and the date and time of data erasure.

Clusterfy also stands ready to aid the Data Controller in responding to data erasure inquiries from data subjects, providing assistance in verifying identification of the requestor and documenting the actions taken in response to the. Clusterfy understands the importance of efficient and compliant handling of such requests is committed to providing full support to the Data Controller in this regard.

Personal Data erasure processes undertaken by Clusterfy will be performed in compliance the applicable standards and regulations, ensuring that Clusterfy's responsibilities and commitment GDPR compliance are upheld throughout the duration and conclusion of the data processing services

9. Sub-Processing

Clusterfy hereby acknowledges and agrees that in the event of any Sub-Processing activities related to use of SynapseGPT by users and businesses, such activities will be conducted with strict adherence to the applicable data protection law and this Addendum.

Clusterfy will provide Clusterfy with a general written authorization to employ sub-processors under this Addendum for the Commissioned Processing. We shall inform Clusterfy, and consequently its users and associated, of any intended changes concerning the addition or replacement of sub-processors thereby affording Clusterfy the opportunity to object to such changes.

Clusterfy objects to any changes in the sub-processing arrangement, Clusterfy make reasonable commercial efforts to secure an alternative sub-processor to which Cluster shall also have the right to object. If an agreement cannot be reached an alternative sub-processor, Clusterfy shall have the right to terminate provision of Services under this Addendum.

Clusterfy shall ensure that sub-processor agreement imposes data protection obligations on the sub-processor which no less onerous than those imposed on

Clusterfy under this addendum, and shall include comparable Technical and Organizational Measures to protect Personal to the standard required by Clusterfy.

Prior to engaging any sub-processor, Clusterfy will perform adequate due diligence to ensure that the sub-processor is capable of providing the level of for Personal Data required by Clusterfy. Upon Clusterfy's request, the written subcontract with a sub- processor will be available for Clusterfy to, to ensure compliance with the standards specified in this Addendum.

Clusterfy fully liable to Clusterfy for the performance of the sub-processor's under the terms agreed upon. In case a sub-processor fails to fulfill obligations regarding data protection, Clusterfy shall promptly take corrective action, but not limited to the termination of the sub-processor's services and Clusterfy of such measures.

Through this process, Clusterfy commits ensuring the protection of Personal Data relating to the use of SynapseGPT and maintains alignment with Clusterfy's commitment to data security and privacy in with GDPR compliance requirements.

10. Monitoring and Audit Rights

At Clusterfy, we recognize the importance of transparency and accountability, particularly when it comes to the handling of personal data within our SynapseGPT platform To this end, we are committed to ensuring robust monitoring and audit mechanisms that align with our established Standard Data Processing Handbook.

We hereby permit and fully support regular audits and inspections by Data Controllers, or any other mandated party as per the applicable GDPR compliance requirements, to verify adherence to the appropriate data protection obligations outlined within our service agreements Such audits shall be conducted by either a reputable and agreed upon independent auditor or, where appropriate by the relevant Data Protection Authority (DPA).

To facilitate these, Clusterfy shall provide all necessary assistance, including granting access to premises systems, documentation, and personnel associated with the processing of personal data under SynapseGPT. All such activities will be conducted in accordance with established policies to prevent any disruption to the operations or compromise of the data being.

Furthermore, Clusterfy shall maintain a comprehensive and accurate record of all processing activities on SynapseGPT, which shall be available upon request to compliance with GDPR and this handbook. Our internal data protection officer (D) will oversee all monitoring and audit activities, serving as the primary contact for auditors and regulatory authorities.

We also acknowledge the requirement to notify Controllers of any substantial legislative changes that might impact our data processing terms or protection measures as specified in our agreements. In instances where such changes affect capacity to fulfill audit compliance, we shall inform the Data Controllers promptly, that appropriate protective measures can be contemplated.

Clusterfy assures that any identified or gaps in compliance from the audit findings will be addressed immediately and rectified in line with GDPR specifications, thus reinforcing our commitment to maintain the highest of data protection and privacy for our clients utilizing SynapseGPT.

11. Data Processor Breach Notification

In the event of a personal data breach involving SynapseGPT by Clusterfy, we as the Data Processor will adhere to the following breach notification procedures, in compliance with GDPR and the Standard Data Processing Handbook guidelines:

1. Incident Identification: Upon discovering any suspected or actual breach of personal data, immediate action will be taken to identify and assess the incident.

2. Containment and Recovery: We will swiftly implement our incident response and recovery plan, aimed at containing the breach, eradicating the, and restoring data integrity and system security.

3. Notification Protocol: In the event that the breach poses risk to the personal data that we process on behalf of our Users or Clients (Data Controllers), we will notify the affected party without undue delay and no later than 72 hours after having become aware of it. Clusterfy will provide details of the breach including the nature of the personal data involved the category and approximate number of data subjects affected, and the category and number of personal data records affected.

4. Contents of Notification: notification to the Data Controller will include:

   - The likely consequences the personal data breach,
   - The measures taken or proposed to be by us to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects,
   - The contact details of our data protection officer or another contact point where more information can be obtained.

5. Communication with Authorities: If the breach is likely to result in a risk to the rights and freedoms of natural persons, we will assist the Controller in communicating the breach to the appropriate supervisory authority prior to notification as required by GDPR Article 33.

6. Communication with Data: When the breach is likely to result in a high risk to the and freedoms of individuals, and where required by law, we will aid the Data Controller in the process to the data subjects, as mandated by GDPR Article 34.

7. Documentation: All personal data breaches will be documented, including the relating to the personal data breach, effects, and the remedial actions taken. This documentation enables the superv authority to verify compliance with GDPR Article 33(5).

8. Continuous Improvement: Following a breach, we will conduct a thorough investigation to the breach's root causes and will put into effect any changes required to systems and practices to prevent similar breaches in the future.

Clusterfy is to maintaining a robust breach notification system and will allocate all necessary resources to the confidentiality, integrity, and availability of personal data that we process. Our is to uphold our obligations under GDPR to the highest standard and to maintain trust that our Users and Business Clients place in our service and our responsibility as a Data Processor.

In the performance of the GDPR-compliant processing activities of personal data, Clusterfy, herein referred as the Data Processor, acknowledges that it may engage Sub-Processors to process personal data on behalf of our clients, known as the Data Controllers.

Clusterfy shall not subcontract any of its processing operations performed on behalf of the Data Controller under the of the General Data Protection Regulation (GDPR) without the Data Controller prior written consent. Where Clusterfy does engage Sub-Processors the consent of the Data Controller, it shall do so only by way a written agreement with the Sub-Processor which imposes the same data protection as set out in the Standard Data Processing Terms and the GDPR. This must provide an equivalent level of protection for the personal data as Clusterfy committed to upholding under the terms of our agreement with the Data Controller.

To onboard any Sub-Processor, Clusterfy shall perform due diligence to ensure that the Sub-Processor is capable and can provide sufficient guarantees implement appropriate technical and organizational measures in such a manner that the processing will the requirements of the GDPR.

Clusterfy shall keep an updated of Sub-Processors and shall provide such list to the Data Controller request, allowing for reasonable notice to object to the appointment of a new-Processor. Objections by the Data Controller shall be submitted in writing a reasonable time period and shall include reasonable grounds related to data protection concerns In the event that a Data Controller objects to a new Sub-Processor Clusterfy is unable to provide a reasonable alternative, the Data Controller may at its discretion, terminate the agreement pursuant to the termination provisions contained thereinIn case of a Sub- Processor's failure to fulfill its data protection, Clusterfy shall remain fully liable to the Data Controller for the of the Sub-Processor's obligations., Clusterfy shall that the contract between it and the Sub-Processor includes a third-party clause that allows the Data Subjects to enforce the terms of the agreement directly the Sub-Processor, should both Clusterfy and Data Controller fail do so.

Upon the termination of the data processing services or upon the of the Data Controller, Clusterfy shall, at the choice of the Controller, return or delete all personal data processed on behalf of the Data by the Sub-Processor, unless EU or EU Member State law requires storage of such personal data.

All Sub-Processor agreements shall be governed the law of the jurisdiction in which

Clusterfy is established and shall be subject the applicable GDPR provisions regarding data processing. Clusterfy commits to being with the Data Controller, providing all information to demonstrate compliance with the obligations set in our Data Processing Agreement.

In accordance with our responsibilities a Data Processor under the General Data Protection Regulation (GDPR) and our commitment to uphold the data protection principles and obligations outlined in the Standard Data Processing Handbook, we at Clusterfy hereby outline the additional obligations we undertake in the processing of Data with regard to the use of SynapseGPT:

1. Compliance with Specific Instructions: We process Personal Data solely based on the documented provided by the Data Controller. In event of any request for data processing outside scope of the provided instructions, explicit from the Data Controller will be sought prior any such processing.

2. Confidentiality and Training: All employees of Clusterfy are granted access to the Personal Data will subject to robust confidentiality agreements. We ensure that our staff are trained in GDPR compliance and the secure and proper handling of Data.

3. Data Subject's Rights: We will assist the Data in upholding the rights of Data Subjects, including the rights to access correction, deletion, portability, and objection of their Personal Data, a timely manner.

4. Sub-processors: Any engagement of sub-processors only be carried out with prior written consent from the Data Controller. We will ensure that any such sub-processors abide by the same data protection obligations as stipulated by the Standard Data Processing Handbook and GDPR.

5. Security Measures: Clusterfy is committed to implementing maintaining comprehensive technical and organizational security measures, as outlined in Annex 1 the Standard Data Processing Handbook, to safeguard Personal Data against unauthorized or unlawful and against accidental loss, destruction, or damage.

6. Data Breach Notification: We will notify the Data Controller without undue delay upon becoming aware any Personal Data breach. We will cooperate fully with the Data Controller in investigation, mitigation, and remediation of any such breach.

7. Data Impact Assessment and Prior Consultation: Clusterfy will provide necessary assistance for performance of any Data Protection Impact Assessments (DPIAs), and consult with the Data Controller regarding any data processing operations that are likely to in high risk to the rights and freedoms of natural persons under GDPR.

8. Deletion or Return of Data: Upon the termination of services involving processing, or upon the request of the Data Controller, we will, the choice of the Data Controller, delete or

return all Personal Data to Controller, and delete existing copies unless EU law or the law of an Member State requires storage of that Personal Data.

9. Record Keeping: will maintain all records required by Article 30 of the GDPR and will such records available to the Data Controller and supervisory authority upon request.

10. Audit and Compliance: Clusterfy will allow for and contribute to audits including inspections, conducted by the Data Controller or auditor mandated by the Data. These audits will ascertain compliance with the obligations set out in this document and the GDPR.

By agreeing to these additional obligations, Clusterfy demonstrates its to the highest standards of data processing and GDPR compliance in the operation and of SynapseGPT for the benefit of our users and partnering enterprises.

14. Third-Party Beneficiary Clause

In recognizing the rights of data subjects as stipulated under General Data Protection Regulation (GDPR), Clusterfy hereby explicitly stipulates that all data subjects whose personal data is processed by SynapseGPT have right to enforce, as third-party beneficiaries, the obligations of {company pertaining to the protection of their personal data against the Data Processor and, where applicable, any Data Sub-Processor.

Data subjects shall have the right to lodge a complaint and pursue remedies as allowed under the GDPR, should they believe that their rights under data processing terms have been infringed as a result of the processing of personal data by SynapseGPT. It should be noted that data may exercise their rights against Clusterfy without prejudice to their rights under GDPR.

Furthermore, if Clusterfy becomes insolvent, ceases business operations, or undergoes any legal transformations affecting its fulfillment of GDPR, the data subjects may enforce their rights against any entity that may assume Clusterfy's legal obligations under this handbook, whether by operation of law through an assumption of contract.

Clusterfy is committed to ensuring such third-party rights are communicated clearly to all data subjects and that these-party beneficiary provisions are incorporated into all contracts with Data Sub-Processors, thereby maintaining a consistent level of data protection as required by Clusterfy and its

15. Annexes and Technical Specifications

Appendix A: Data Processing Specifications

This appendix forms an integral part the data processing and GDPR compliance guidelines implemented by Clusterfy the operation of SynapseGPT, ensuring its adherence to the latest standards for personal data protection and processing.

1. Purpose of Data Processing

The SynapseGPT platform data to provide users with AI-driven solutions, but not limited to, document analysis, text generation, and systems integration. Clusterfy personal data to extent necessary to fulfill these purposes while complying with GDPR requirements.

2. Personal Data Processing

The processing of personal data shall continue for as long as necessary to provide the requested services to users or until consent is withdrawn by individual data subjects, all in accordance with the terms of the service agreement and GDPR provisions.

3. Categories of Data Subjects

The platform may handle personal data pertaining to:

- Employees of Client companies using SynapseGPT.
- Clients and their customers who directly interact with SynapseGPT.
- Any individuals whose data is processed as part of the provided through SynapseGPT.

4. Types of Personal Data Processed.

The types of personal data processed by SynapseGPT include:

Names and contact information of users (email addresses, phone numbers). Professional titles and roles within the businesses.

- Usage data, such login credentials, usage patterns, and user preferences.
- Other personal that may be required to provide the services.

5. Data Processing Operations. Clusterfy, through the use of SynapseGPT, may carry various operations on the data, including:

- Collection and storage of data for the provision of services.
- Analysis and processing of content for delivery and improvement.
- Anonymization or pseudonymization where to enhance privacy.
- Periodic deletion of data in accordance with policies and data subject requests.

6. Data Protection Measures

Clusterfy to the implementation of the technical and organizational measures as outlined in Annex 1, including encryption, access control, and secure data transfer protocols to protect integrity and confidentiality of the personal data7. Sub- Processors

Cluster may engage sub-processors to perform certain tasks on behalf of Clusterfy. sub-processors are contractually bound to provide at least the same level of data and privacy as set forth in Clusterfy's terms and within the scope of GDPR.

7. International Data Transfers

Any transfer of data outside the European Economic (EEA) will be carried out in compliance with Chapter V of the GDPR. Clusterfy shall employ appropriate safeguards, such standard contractual clauses, for all international data transfers.

Appendix B: Technical and Organizational Measures

Clusterfy undertakes various actions to ensure the confidentiality, integrity and availability of personal data processed through SynapseGPT. These include, but are not limited to:

- The deployment of secure server infrastructure firewall protection and intrusion detection systems.
- Regular security audits and penetration performed by qualified third-party experts.
- Employee training programs focused on privacy, cybersecurity, and incident response.
- The establishment of robust recovery and backup processes to handle potential data loss scenarios effectively.

For a outline of our full Technical and Organizational Measures, please refer to Annex1 to the Data Processing Addendum provided as part of our data protection with users and clients.

15.1. Detailed Security Measures

At Clusterfy we have established and implemented the following detailed security measures that align with the technical and organizational requirements outlined in the Standard Data Processing Handbook:

1. Access Control: We use sophisticated role-based access controls to ensure that only authorized Clusterfy personnel have access to personal data. Access logs are maintained and regularly reviewed for any unauthorized access attempts.

2 Data Encryption: All sensitive information, including data, transmitted to or from SynapseGPT is encrypted using state-the-art cryptographic protocols. Data at rest is also stored in encrypted formats prevent unauthorized access and data breaches.

3. Network Security: Our networks secured with firewalls, intrusion detection systems, and regular penetration testing to and mitigate vulnerabilities. SynapseGPT’s infrastructure is protected against network.

4. Data Minimization: We process and store only the minimum of personal data necessary for delivering the SynapseGPT services, in line the principles of data minimization.

5. Regular Audits: We regular audits to ensure our data processing activities are in compliance with GDPR and relevant data protection regulations. Findings from are addressed promptly to maintain integrity and security.

6. Personnel Training: Our team members are trained on the of data security and privacy. They are required to understand and fully comply all policies regarding data protection, ensuring that our organization maintains high standards of privacy.

7. Sub-processor Oversight: In cases where third-party service are engaged as subprocess, we ensure that they also abide by GDPR-compliant security measures and enter into contractual terms that reflect the responsibilities and obligations involved in processing personal data.

8. Incident Response: We have established an incident response plan to react quickly and effectively to any breach. This includes immediate measures to mitigate the impact, followed by a thorough, and necessary notifications to supervisory authorities and affected individuals within the timeframe by law.

9. Data Integrity and Transfer: Mechanisms are in to ensure the integrity of personal data during transmission, handling, and storage Data is not transferred to countries outside the European Economic Area without ensuring adequate levels of data protection.

10. Data Retention and Disposal: We adhere to defined data retention policies that comply with legal obligations. Data is of securely when no longer needed or when requested by the individual concerned.