### **Between:**

**The Client**,

**And:**

**Whereas:**

Client wishes to use a communication platform for its website (hereinafter: 'communication platform'), developed by XXX.me.

1. Client and XXX.me have entered into an Agreement for this purpose.
2. Under that agreement, XXX.me processes personal data obtained by Client.
3. The agreements made between Client and XXX.me about the processing of the Personal Data are set out in this Processing Agreement.
4. In addition to the provisions of this Agreement, the Parties agree as follows in the light of Article 28, paragraph 3 of the General Data Protection Regulation (GDPR).

### **Article 1. Definitions**

In this Processing Agreement, the following terms, always referred to with a capital letter, both in singular and in plural, have the following meaning:

1. GDPR: General Data Protection Regulation;
2. *Data Subject:*  The identified or identifiable natural person to whom the Personal Data relates, as referred to in Article 4 under 1 GDPR;
3. *Processor:* The Processor as referred to in Article 4 under 8. GDPR. In this Processing Agreement: XXX.me;
4. *Processing Agreement:* This Processing Agreement, which is an integral part of the Agreement, for setting out the agreements referred to in art. 28 paragraph 3 GDPR;
5. *Agreement*: The agreement between the Client and XXX.me including appendices, for the use of the communication platform.
6. *(Data) Breach:* a security breach that inadvertently or unlawfully leads to the destruction, loss, modification or unauthorised provision of or unauthorized access to transmitted, stored or otherwise processed data;
7. *Parties*: Client and XXX.me;
8. *Personal Data*: data which relates to an individual and which identifies that individual, either directly or indirectly, as referred to in Article 4 under 1 GDPR;
9. *Controller*: The controller as referred to in art. 4 under 7. GDPR. In this Processing Agreement: Client;
10. *Processing*: Any operation or set of operations relating to Personal Data including collecting, recording, organizing, storing, updating, modifying, retrieving, consulting, using, providing by means of forwarding, distribution or any other form of proving, bringing together, connect, as well as the protection, deletion or destruction of Personal Data, as referred to in art. 4 under 2 GDPR.

### **Article 2. Duration and termination**

2.1 This Processing Agreement commences at the time of signing and continues as long as XXX.me acts as a Processor of Personal Data, within the framework of the Personal Data provided by the Client, in the performance of the work, as described in the Agreement.

2.2 As soon as the collaboration has ended, XXX.me will either, demonstrably erase all Personal Data within one month of the termination date or return it to the Client, and evidently delete existing copies, whichever the Client prefers, unless Parties agree otherwise or when storage of the Personal Data based on rules and regulations is mandatory. Client may, if deemed necessary, impose further requirements on the manner of return or the destruction, including reasonable requirements regarding the file format.

2.3 XXX.me will at all times guarantee the data portability in the execution of the provisions of the previous paragraph in such a way that there is no loss of functionality or (parts of) the data.

### **Article 3. Scope of Processing Agreement and Processing by XXX.me**

3.1 XXX.me will Process the Personal Data made available by or through the Client, solely on behalf of the Client, for the performance of the Agreement.

3.2 Client sets out the purposes for the Processing of Personal Data. XXX.me Processes Personal Data on behalf of the Client exclusively for the purpose of facilitating the communication platform.

3.3 XXX.me will not Process the Personal Data for any other purpose set out by the Client.

3.4 XXX.me Processes the data only within the European Union.

3.5 XXX.me has no control over the provided Personal Data. For example, XXX.me does not make decisions about receipt and use of the data, the provision to third parties and the duration of the storage of data. The control over the Personal Data provided under this Processing Agreement shall never be vested in XXX.me.

 3.6 XXX.me will act, for purpose of the Processing of Personal Data, in accordance with the applicable laws and regulations regarding the Processing of Personal Data. XXX.me will follow all reasonable written instructions from Customer, subject to deviating legal obligations.

3.7 XXX.me shall at all times provide Client with the Personal Data made available by Client under this Processing Agreement at Client's initial request.

3.8 XXX.me is solely responsible for the Processing of Personal Data via the service offered by it in the Agreement, under the conditions stated in the Processing Agreement. For the other Processing of Personal Data, including but not limited to the collection of the Personal Data by Customer and/or third parties, XXX.me is explicitly not responsible.

### **Article 4. Security**

4.1 XXX.me shall ensure an adequate level of security of the Personal Data it Processes against misuse and unauthorized use.

4.2 Parties agree that XXX.me will implement all appropriate technical and organisational measures to protect the Personal Data that will be Processed against loss or against any form of unlawful Processing (such as unauthorized access, impairment, alteration or provision of the data). The methods of security are described in more detail in the Security Protocol in the appendix.

4.3 XXX.me guarantees to have at least taken the measures mentioned in the Security Protocol, which has been established in consultation between Parties and which is attached to this Processing Agreement. XXX.me may only amend the Security Protocol if Client agrees to the adjustment prior to the change and if the level of security is not reduced.

**Article 5. Audits**

5.1 Client has the right to have compliance under this Processing Agreement inspected by an auditor at any time.

5.2 XXX.me will store the supporting data required for the audits, including system logs.

5.3 The persons conducting the audit will abide by the security procedures at XXX.me.

5.4 XXX.me will comply with the audit and make available all information reasonably relevant to the audit in a timely manner.

5.5 XXX.me guarantees to implement the reasonable recommendations suggested by Client or engaged third party for improvement, within a reasonable time frame, which will be determined in consultation.

5.6 The costs of an audit shall be borne by Client.

5.7 Client will not commence an audit earlier than 14 (fourteen) days after prior written notice. If the date and time of the audit does not suit XXX.me, then XXX.me will inform the Client of this and propose a new date.

5.8 XXX.me undertakes to provide Client, or a third party engaged by Client, with the requested information within a timeframe determined to by Client. This way, Client, or a third party engaged by Client, can form an opinion regarding XXX.me's compliance of this Processing Agreement. Client, or a third party engaged by Client, is obligated to treat all information concerning these checks confidentially.

### **Article 6. Indemnities**

6.1 XXX.me shall indemnify Client against any third party legal claims, on any grounds whatsoever, with regards to the Personal Data or the fulfilment of the Processing Agreement and/or Agreement, unless XXX.me proves to have taken all technical and organisational measures to protect the Personal Data as described in the appendix to this Processing Agreement and has also, for the remainder, not acted unlawfully which resulted in the damage.

6.2 If the third party legal claims regarding the Personal Data or the fulfilment of the Processing Agreement and/or Agreement are the result of intent or gross negligence by XXX.me, then XXX.me will indemnify the Client at least with respect to those relevant legal claims.

### **Article 7. Confidentiality**

7.1 All Personal Data that XXX.me receives from Client and/or collects or has to collect for the purpose of Processing the data in accordance with the provisions of the Agreement, is subject to confidentiality towards third parties. People employed by or working for XXX.me will sign an associated confidentiality agreement.

7.2 XXX.me will not use this information for any other purpose than for which it has obtained it, even if it has been altered in such a way that it cannot be traced back to Client or any other person, such as the Data Subject.

7.3 Ensuring confidentiality does not apply if the Client, or the Data Subject, has explicitly given permission, or in case there is a legal obligation to provide information to a third party.

7.4 If XXX.me uses the services of third parties, it unconditionally ensures that these third parties will accept in writing and comply to the same confidentiality as agreed to between Parties.

7.5 If XXX.me has to provide data based on a legal obligation or court order, XXX.me will verify the basis of the request and the identity of the inquirer and XXX.me will immediately, prior to the provision, inform Client, unless legal provisions impede this.

### **Article 8. Duty to report**

* 1. In the event of a Breach, XXX.me will inform Client as soon as possible - at least within 24 hours after the first discovery - of all (suspected) security breaches and other incidents that must be reported under the law, to the authorities or Data Subject as far as the Breaches are related to Client's Processed data. This without prejudice to the obligation to undo or limit the consequences of such Breaches and incidents as quickly as possible. XXX.me will additionally, at the initial request of Client, provide all information that Client deems necessary to be able to assess the event. XXX.me will provide at least the information about the (alleged) cause of the Breach and the (proposed) solution.

8.2 XXX.me has a thorough plan of approaching and dealing with Breaches, and will provide the Client, at his request, with access to that plan. XXX.me notifies Client of any substantive changes to the plan.

8.3 XXX.me will leave it to Client to report Breaches to the authorities. Such a report by Client shall in itself never be regarded as a shortcoming in the fulfilment of this Processing Agreement or the underlying main agreement or otherwise as an unlawful act. XXX.me will support Client with reports to Data Subjects and/or authorities.

8.4 XXX.me keeps a detailed log of all (suspected) Security Breaches, as well as the actions taken as a follow-up to such Breaches and gives access to this log upon Client's initial request.

8.5 XXX.me will provide all necessary assistance to Client so that it can provide (additional) information to authorities and/or Data Subject(s) in the shortest possible time.

### **Article 9. Data Subject Rights**

XXX.me enables Client at all times to comply within the legal time frames with the obligations under the GDPR, in particular the rights of Data Subjects, including, a request for access, correction, supplementation, removal or protection of Personal Data and the performance of an acknowledged registered objection.

### **Article 10. Engaging third parties**

10.1 Client has given XXX.me permission to engage third parties in the context of the fulfilment of the Processing Agreement.

10.2 XXX.me is fully responsible for this third party and it will impose at least the same obligations on to the third party relative to the Client as those arising from this Processing Agreement. If a third party fails to meet its obligations, XXX.me will remain fully liable to Client for the fulfilment of the obligations under the Processing Agreement.

10.3 XXX.me informs Client about intended changes regarding the addition or replacement of other Processors. Client has the opportunity to object to these changes.

### **Article 11. Liability**

11.1 XXX.me is liable for damage or loss resulting from non-compliance, late or improper performance of the Agreement and/or this Processing Agreement.

11.2 Client is liable for all damage or loss resulting from the non-fulfilment of the Agreement and/or this Processing Agreement, unless the non-compliance cannot be attributed to Client.

11.3 If a Party imputably fails to fulfil an agreed obligation, the other party may give notice to the negligent party which will include a reasonable period for performance. Does fulfilment still not occur, then the negligent party is in default. A default notice is not necessary if compliance with a strict deadline applies, fulfilment is permanently impossible or if it should be interpreted from a statement or from the behaviour of the other party that it will fail to fulfil its obligation.

11.4 Client may, without prejudice to the provisions of the Processing Agreement and the related Agreement, and without prejudice to the provisions of the law, suspend the fulfilment of this Processing Agreement by means of registered post, or without legal intervention, with immediate effect, fully or partially terminate if Client ascertains that:

1. XXX.me applies for a moratorium; or
2. XXX.me files for bankruptcy or is declared bankrupt; or
3. XXX.me is being wound up; or
4. XXX.me ceases business; or
5. there is a significant change in the governing of activities of the XXX.me company, which means that it cannot reasonably be expected of the Client that the Processing Agreement be continued; or
6. a substantial part of the assets of XXX.me is seized (other than by Client); or

g) the other party verifiably fails to perform the obligations arising from this Processing Agreement, and that failure has not been rectified within a reasonable period, after a written notice to that effect, or one of the other situations referred to in Article 11.3 occurs.

11.5 XXX.me informs Client immediately if a bankruptcy or moratorium is likely to happen, so Client can decide in a timely manner whether to recover the Personal Data.

Client is entitled to terminate this Processing Agreement immediately if XXX.me indicates that it is no longer able to meet the security requirements which are, based on developments in the law and/or jurisprudence, relevant to the Processing of Personal Data.

### **Article 12. Dispute settlement**

12.1 To the Agreement and this Processing Agreement, as well as to the resulting or related agreements and other legal acts, Dutch law applies exclusively.

12.2 All disputes, including those which are only regarded as such by one party, shall be settled by the appropriate court in the district where XXX.me is located.

### **Article 13.**

The Processing Agreement is part of the Agreement. In the event of a conflict between the Agreement and the Processing Agreement, the provisions of the Processing Agreement shall take precedence.

**Article 14. Amending the Processing Agreement**

14.1 Amendments to this Processing Agreement can only be made in writing by means of a proposal approved by both Parties.

14.2 Controller and Processor enter into consultation with each other about changes to this Processing Agreement if a change in regulations or a change in the interpretation of regulations bring this about.

|  |  |
| --- | --- |
| **For approval, XXX.me:** | **For approval ,Client:** |
|  |  |  |
| Name: | J.G, Arens |  | Name: |  |
| Date: |  |  | Date: |  |

**Appendix**

**XXX.me Security Protocol**

# Purpose and background of this document

Pursuant to Article 32 of the GDPR, Client is obliged to implement appropriate technical and organisational measures to protect Personal Data against Data Breaches. According to the law, the measures, taking into account the state of the art and the costs of implementation, must ensure a suitable level of security appropriate to the risks of Processing and the nature of the to be protected data entail. The measures must be inter alia aimed at preventing unnecessary collection and further Processing of Personal Data.

Based on Article 28 of the GDPR, Client must ensure that persons who process Personal Data on behalf of Client, such as XXX.me, also implement appropriate technical and organisational measures.

This Security Protocol is an appendix of the Processing Agreement between Client and XXX.me and determines the technical and organisational measures that XXX.me ensures to implement as Client's Processer.

This Security Protocol contains sensitive information regarding the security of the communication platform and the handling of personal data. If unauthorized people take note of this information, it poses a great risk. Therefore, this Security Protocol must be treated strictly confidential.

# Organisational security measures

## General organisational measures

XXX.me's Security Officer is (ultimately) responsible for information protection and ensures that the technical and organizational security measures are adhered to and that this can clearly be verified. Below is an overview of the agreed security measures.

## Preventive measures[[1]](#footnote-1)

### Only persons who, because of their position, have a legitimate need for the Processing of Personal Data, will receive the means and data required to gain access to the Personal Data (through physical or digital means).

###  All employees who process Personal Data are properly informed about which forms of Processing are permitted and which are not. The employees in question have at least received and read this Security Protocol.

### Information with which access can be obtained to Personal Data, such as user names, passwords and tokens or smart cards, are carefully stored by the person to whom they have been provided.

### Persons who have a personal interest in certain Personal Data, other than just for the performance of their job, which are processed in the systems (servers/applications), do not have access to those systems, unless the relevant Personal Data is protected in such a way that it is impossible for these persons to gain access to the Personal Data, even if they do have access to the systems.[[2]](#footnote-2)

## Detective control[[3]](#footnote-3)

### XXX.me's Security Officer regularly checks at random (and as discreetly as possible, taking into account a reasonable level of privacy for employees) whether employees take the measures that they're expected to take and do not carry out unauthorized Processing or cause Data Breaches.

### Employees who (might) have caused a Data Breach by failing to take the right measures and who report this in a fair and timely manner to the manager and/or Security Officer will receive lighter sanctions.

## Mitigating and recovery measures[[4]](#footnote-4)

### As soon as someone in the organization knows of a (possible) Data Breach with potential harmful consequences, this person must inform the Security Officer.

### The Security Officer ensures that, if necessary, the right people outside of the company are informed about the Data Breach in a timely manner. At least the project manager at XXX.me must be informed.

### The Security Officer is in charge and, where necessary, assigns tasks and responsibilities to other employees to limit damages as a result of a Data Breach as much and as quickly as possible and to prevent similar Data Breaches from happening in the future.

## Corrective measures[[5]](#footnote-5)

### The employment contract, work regulations and/or confidentiality agreement contains sanctions for violating confidentiality or non-compliance with security protocols. The sanctions are proportional to the severity of the violation.

### Meetings are held periodically with the appropriate employees to evaluate the effectiveness and proportionality of measures that have been taken and, if a Data Breach has occurred, to learn from that and to invoke more stringent measures.

# Technical security measures

## General technical measures

### XXX.me should take note of all security measures recommended by the developers of the used (open source) software packages for information security purposes. The 'apply-or-explain' principle applies to every recommended measure. Every measure should in principal be implemented and only if there is a more serious reason not to do so, can this be disregarded.

## Preventive measures

### The following security measures apply to all servers (computers) that are accessible from the Internet and Process Personal Data.

### Areas with servers that Process Personal Data are only accessible for authorized personnel. For servers that Process Personal Data, the area is supplied with an automatically closing door, which can only be opened with the correct physical, magnetic or biometric key.

### Remote access to the Personal Data servers is made safe with secure passwords and/or tokens. The software that enables the remote access contains measures against 'brute force' attacks, such as limiting the number of possible log-in attempts per set timeframe and 'blacklisting' of IP addresses with which excessive amounts of log-in attempts are made.

### Passwords used to authenticate persons who are authorized to Process Personal Data are adequately long and not easy to guess. This will be in line with current guidelines on safe passwords[.](http://www.microsoft.com/nl-nl/security/online-%09privacy/passwords-create.aspx)

### The software on the servers is carefully kept up-to-date via a reliable patch management process.[[6]](#footnote-6)

### If the server is used for the Processing of Personal Data, it will only be used to carry out the intended Processing and not for any other tasks.

### The services offered by the server must be authenticated ensuring that only authorized users have access to the services.

### All access to Personal Data must be recorded (logged). When logging the access, at least the date, time (including time zone), the authorized user and the description of the obtained access must be recorded.

### Data are Processed anonymously as much as possible and stored no longer than necessary.

## Detective measures

### An up-to-date virus scanner has been installed on the server from a brand considered to be reliable.

### We use properly configured firewalls.

### Servers on which Personal Data is Processed are equipped with software designed to detect and prevent attacks.

## Mitigating and recovery measures

### There is a procedure for restoring lost Personal Data with the help of backups (restore procedure). The restore procedure is tested regularly, and organised in such a way that the period between the moment a backup is made and when its used for recovery is never more than one day.

## Corrective measures

### When a Data Breach has occurred, the Security Officer will investigate what the most important technical causes of the Data Breach have been. The technical procedures are adjusted in such a way that the identified technical causes cannot lead to a Data Breach again.

# Complete list of actual security measures

The security can be divided into a number of components:

1. Physical security of the servers
2. Electronic security of the servers
3. Software related security
4. Internal security measures XXX.me
5. User management
6. Backup locations

## Physical security server park

All servers are set up in a 24-hour secured location. The security includes access cards and staffed video surveillance. Access is not possible without approval, identification and checks. The servers are placed in a rack with a code lock. Access is granted only to employees of the provider (LeaseWeb) and only when this is necessary.

## Electronic security server park

Of all the servers in the network of the provider, the BIOS is protected with a password. It cannot be started from any medium other than the hard disk. Together, the servers form a cluster which is managed exclusively by employees of the provider. Access to the cluster is only possible through a secure connection.

## Security server

The server uses Linux Ubuntu as the operating system. Updates are automatically applied.

Remote access to the server is only possible over the TCP ports 25, 53, 80, 110 and 443.

Some other ports are only accessible from LeaseWeb management locations.

The number of Linux users on the server is kept to a minimum and rights are only granted to the users for whom this is strictly necessary. A 'difficult' password has been set for all users.

## Security source code

A number of safety constructions have been cogitated in the source code of the XXX.me software.

These are general principles on which all code supplied by XXX.me is checked:

* All input is checked for the correct type. This way, incorrect, unsafe input is seized.
* Errors are not shown to the user.
* Everywhere, SQL injection is checked for both writing and retrieving data.
* Session Hijacking is aimed to be prevented by additional checks outside the SESSIONID. The SESSIONID is re-generated after logging in.
* In the event of errors, an error report will be written up immediately and a notification sent to XXX.me (by email). Hack attempts are therefore quickly exposed.
* It is not technically possible for users to view data that they are not allowed to access. A strict separation between user data is guaranteed.

## Organisational measures within XXX.me

* Passwords to access the servers are only provided to employees if this is necessary.
* All employees have signed a confidentiality clause in case they come into contact with (possible) sensitive information.
* Employees only have access to a part of the database (copy) if there is a need for it.
* When using the database for development, Personal Data is made anonymous.
* When using the database for development, all data relating to security is deleted.
* After use for development, the local copy is removed.

##  User management

An encryption algorithm "bcrypt" ensures that user passwords cannot be retrieved, hacked or guessed.

## Backup locations

There are backups stored at the server park of the provider. These are only accessible for repair works and can, if necessary, be used anonymously for development purposes.

## Monitoring / Security notifications

With every incident in a call, a detailed email is automatically sent to Chanenl.me. This message contains all relevant information regarding the fault. This allows for hacking attempts to be easily detected. Hacking attempts are also immediately visible this way.

## Security source code

The provider ensures to make the communication platform as safe as possible. Below features give an indication of the requirements for the development of components. **g**

|  |  |
| --- | --- |
| **One-off authentication:** | The authentication takes place via a secure connection. After logging in, there's a check done for every call. |
| **one-way password encryption:** | Passwords cannot be traced from database or other sources. |
| **Security at module level:** | The security at module level ensures a good separation |
| **Security at IP level:** | If necessary, certain functionalities can be limited by IP addresses. |
| **Data level security:** | If possible, it will also be determined at data level, who has access to certain information |
| **Adjustable number of maximum log-in attempts** | With monitoring at the front, corruption attempts can be detected early |
| **Error reports** | No critical error messages are displayed to the user |
| **Hack-reports** | Attempts by hackers can usually be detected. These are immediately reported to the administrator and an automatic blockage can be put in place. |
| **Shadow database** | All changes to the XXX.me software are registered by name. This means that a loss of data can be limited and we can always look back at who made a change. |
| **Automatic logout:**  | By specifying an expiry time, the user is automatically logged out after a certain period of inactivity. |
| **Access via SSL:** | It can be imposed at the source code level that the XXX.me software can only be accessed via SSL. |
| **Registration of users:**  | Usage of the communication platform and attempts to log in are recorded. |

1. Primarily for knowing that a Data Breach occurred. [↑](#footnote-ref-1)
2. It can not be fully guaranteed that someone will not have access to confidential data from someone who knows this person. This information must be treated strictly confidential and may not be used any way detrimental to the person concerned. [↑](#footnote-ref-2)
3. Primarily for knowing that a Data Breach occurred. [↑](#footnote-ref-3)
4. Primarily for limiting the negative effects of Data Breaches. [↑](#footnote-ref-4)
5. Primarily for repairing shortcomings in security that have led to or could probably lead to Data Breaches [↑](#footnote-ref-5)
6. As stated in article 2.3 of the hosting contract. [↑](#footnote-ref-6)