|  |
| --- |
| Company: AlwaysNext2You |
| Data Protection Impact Assessment (DPIA) |

|  |
| --- |
| Controller: Serafim Ciobanu  08.04.2024 |

Table of Contents

[Introduction 2](#_Toc164196344)

[Data Captivation 2](#_Toc164196345)

[Processing activities 3](#_Toc164196346)

[Dataflow 3](#_Toc164196347)

[Rights of data subject and lawfulness of processing 8](#_Toc164196348)

[Risk mitigation 9](#_Toc164196349)

[Cookie statement 11](#_Toc164196350)

[What are cookies? 11](#_Toc164196351)

[Why do we use cookies? 11](#_Toc164196352)

[Cookie consent 12](#_Toc164196353)

[Cookie duration 12](#_Toc164196354)

[Cookie handling 12](#_Toc164196355)

[Legal compliance 12](#_Toc164196356)

[Updates to the cookie statement 12](#_Toc164196357)

[Contact us 13](#_Toc164196358)

[Appendix 14](#_Toc164196359)

# Introduction

AlwaysNext2You is embarking on the implementation of a digitalized support system aimed at enhancing study support for teenagers through a dedicated website with a customer portal. In accordance with the General Data Protection Regulation (GDPR), this Data Protection Impact Assessment (DPIA) serves to elucidate the processing activities involved, the lawful handling of personal data, the rights afforded to data subjects, risk assessments, the cookie statement, and the data flow pertaining to this initiative.

The envisioned digital platform seeks to capture details about students, including their academic progress, evolution, and contact information, with the overarching goal of providing tailored support services. As teenagers represent the primary target audience, it is imperative to ensure that all data processing activities adhere strictly to the principles of data protection and privacy as outlined in the GDPR.

This DPIA will comprehensively analyze the proposed processing activities, evaluate their compliance with GDPR regulations, assess potential risks to data subjects' privacy and rights, and propose mitigating measures to safeguard against such risks. Additionally, it will address the management of cookies, ensuring transparency and user consent in accordance with relevant regulations.

By conducting this DPIA, AlwaysNext2You demonstrates its commitment to responsible data handling practices and endeavors to establish a digital support platform that not only enhances educational outcomes but also prioritizes the privacy and security of its teenage users' personal information.

# Data Captivation

Since the project is aimed at processing personal data of teenagers, there is a need to specify what kind of information (personal data) is going to be processed, and the purpose of the processing.

As part of our compliance with the General Data Protection Regulation (GDPR) Article 5, we have outlined the categories of personal data to be collected and their respective purposes for processing:

Personal data to be collected

* Last name
* First name
* Gender
* Date of birth
* Student ID
* Institution
* E-mail address
* Phone number
* Parents phone number

The primary goal of the above list is aiming to minimize the amount of information about the student while also getting as much possible insight about the student for a proper support journey, and gathering the upmost information.

Date of birth, gender, last name, and first name are all necessary information to have a complete picture of the student. This information ensures a more cordial relationship between the supporter and the client by facilitating personal approaches hesitant to discuss communication and support, especially in situations where students may be hesitant to share their emotions in public, or even to other people in general.

Student IDs and institutional information are crucial for tracking students' academic achievements. It enables the creation of distinctive learning routes that support and mentor students as they progress through their academic careers and is based on gaining information from the institution itself, rather than gathering it from the student personally.

E-mail address, phone number, and parents’ phone number is necessary to be collected as it is one of the first means to contact the student personally, for a more approached discussion, and a faster way to contact the student. Parents’ phone numbers are necessary for situations where the student is rather hesitant to share information with anyone, and there is a need for internal support, which is mostly coming from the parents.

As a matter of fact, it is important to specify that there is no need for the processing of any special category data for the case of our company.

# Processing activities

Taking into consideration the information regarding the processing of the personal data of students in the previous section, there is a need to specify more information regarding the lawfulness of processing for the data itself, as to give more transparency over the cause.

The controller of the company AlwaysNext2You is represented by the company itself, as the company is processing the information on its own behalf, hence there is no need for any additional processors. The data is not planned to be transferred internationally or to any third-party organization. The processing actions are not occasional and are required to fulfill the capabilities and services offered by the company.

The information is going to be collected via an online form from the digital platform, and stored in the databases that are in the company’s possession, and additionally stored via backups on a second instance. The data related to students’ achievements will be gathered by requests to the related institution. The data will be retained for an additional time of 2 years after the client finishes working with the company. The lawfulness of processing will be based on the consent of the student, if the age is 16 or older, or alternatively the consent of the parents, for those who do not fall under processing rules.

# Dataflow

Considering the already mentioned information regarding the processing of personal data, there appears a need to additionally draw attention towards the flow of data in the company’s system, which is additionally meant to conform with the Art. 25 of GDPR, where we make sure that we implement the best practices for data privacy.

First, it is necessary to define a legend for components that are going to be used in the dataflow diagram. Hence, we will make sure that the diagram is as clear as possible and brings the best understanding of the system, so as to avoid the most part of the misunderstanding of the workflow.

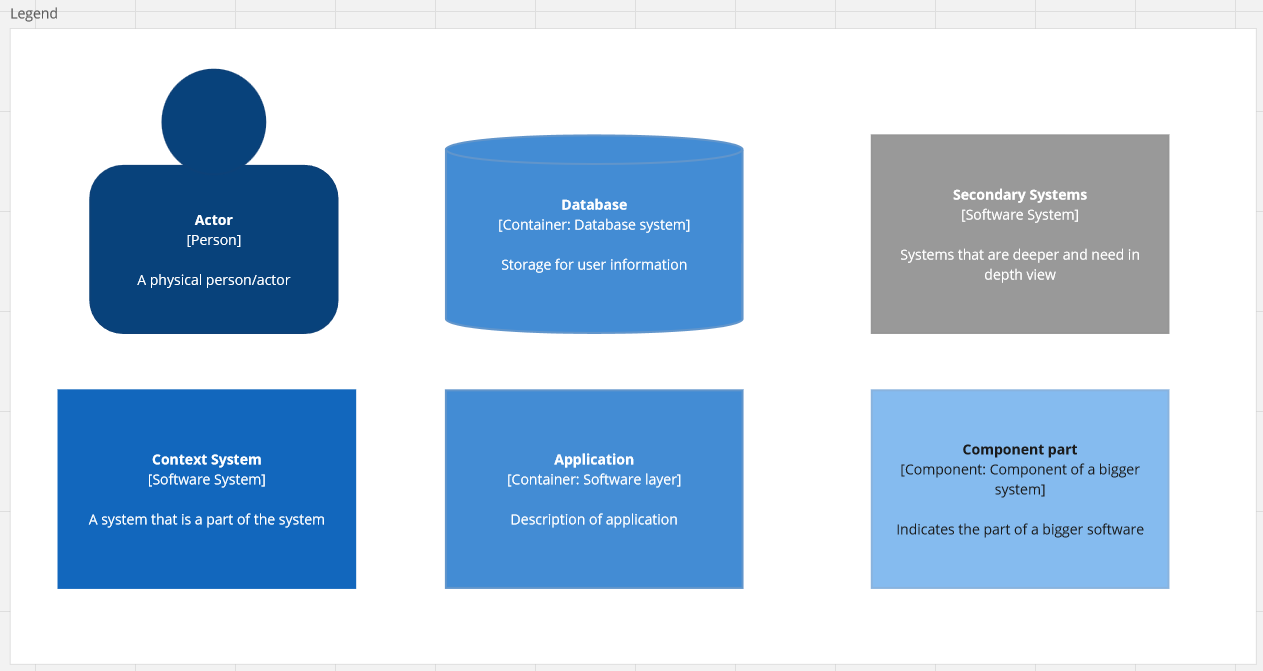


Figure 1: Legend for dataflow.

In the picture above, we mark the main components that are important for the different layers of view of our system, as there will be multiple layers of view, one of them making a clear view of the system with small details, then a more in-depth view of the software that is going to be used, and an in-depth view of a separate system of a component part.

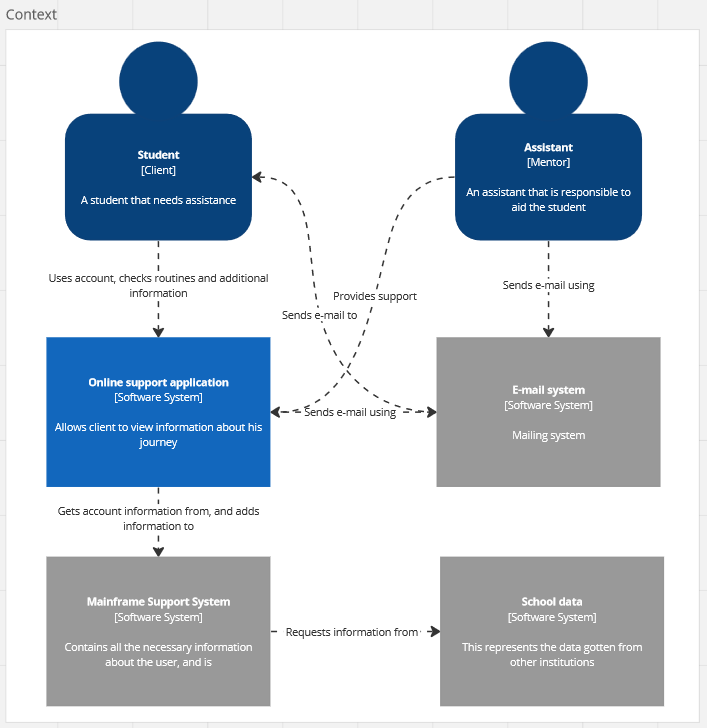


Figure 2: Context diagram.

In the image above, we specified a small overview of the system as a whole. In this diagram, we specified a Context diagram, that has the main objective to show the main component parts that are responsible for making everything work.

Main actors of the system are considered the Mentor (in our case, a helper, whose role is to offer help and support for the client), and the Client (in our case, the teenage himself, that is seeking support in our system). The Client can access the online system, and as the main regulatory and registration login is going to be used the student’s personal email address. Assistant can contact the Client either by the use of the personal email address, or by the means of the platform itself, which is the most preferred method, as personal emailing can be intrusive and used only in upmost necessary cases, or personalized offers.

Other parts of the system, which are Online support application itself, is responsible for managing all the information that is coming from and into the system and be a bridge between the client and the other management sub-systems.

Other parts that are not really talked about are the Mainframe Support System, E-mail system, School data, as they can be diverged and set up based on the company’s needs or be changed based on the objectives of the system. Mainly, the School data component is the evolution of needed data, that should be requested by the company from other institutions, hence gathering the idea about the students’ result. This will ensure that our company does not handle the data only on our behalf, and hence we do not request full access to the other data. The mailing system is dependent on the company and requires a separate server that is responsible for sending and receiving emails as a part of the system. It can be issued by the company itself or used as a cloud provider service. Mainframe Support System is responsible for containing the most interactions on a software level and requires implementation of technical support.

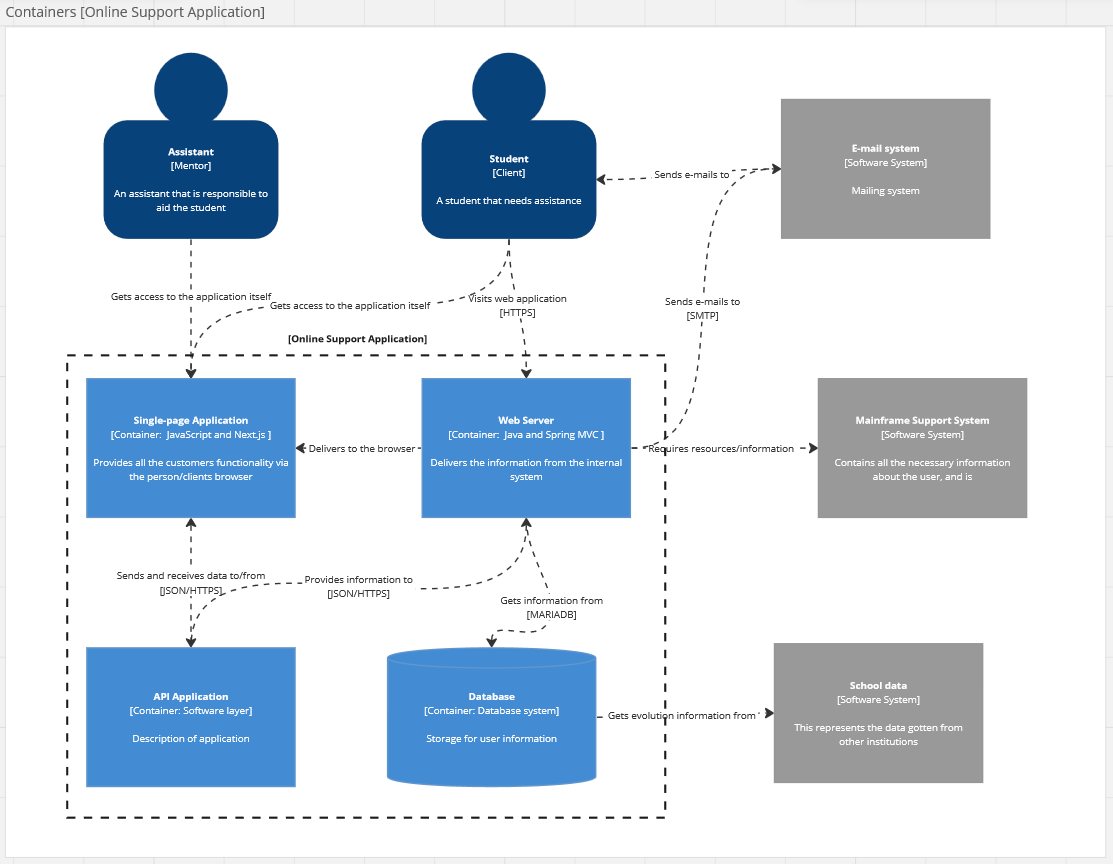


Figure 3: Containers [Online Support Application element]

In the figure above, it is specified more information regarding a crucial part of the whole dataflow, that being the Online Support Application, as it represents the whole grail of what is (one of) main goals of this whole engagement with the company. Other systems are still resembled as greyed out, as they are not particularly important, or play an important role in the design of privacy of the users’ data. As the main idea is to provide the best privacy possible according to the mentioned article at the beginning of chapter.

The controller is responsible for ensuring that the means of transferring data is as secure as possible, and hence, the technical part is going to make use of the most secure technologies and implementations available for the current moment and possibilities. It is also necessary to mention once again that the main focus additionally lays on the data minimization from the company’s side, and minimal processing of the data itself, as most of the manipulations are going to be done manually and not via a usage of a sophisticated machinery that will make the support providing much more digitalizvaed. However, one important point of attention is the fact that we need to provide a pseudonymization instruction for the data storage, which means that the data that is going to be stored on the local databases, and made sure to be split, encrypted (where possible), and stored in such a way that it is not clear what it is from the first time. Since a database is one of the most primarily needed components of the system, we need to make sure that the access to it is not compromised, hence there will be a need for proper sophisticated methods of accessing it, for example – via separated, regulated users from the technical implementation part. This will ensure that even breaking through one layer of protection of a potential threat will not lead to the system totally falling apart and will allow to get a reaction time before the system is totally corrupted. Additionally, it is important to make sure that the communication with the database, and the layers in between is obscure, so that the data can not be clearly understood from the response, and obscured after the receiving of it, in the other layers of the system.

Other layers play the role of a bridge that ensures the digitalized platform an easy to implement solutions and well-known structure. Most of the processing is going to be done on the Web Server component, and a smaller part of it (being some part of validation) on the Single-Page Application. The other data is getting fetched from the database itself, which is maintained separately. Other parts are not that needed to be elaborated further on, as those can have various implementations and depend on the client needs, or the system needs.

A screenshot of a computer screen

Description automatically generated

Figure 4: Components [API Application]

The above image represents the most detailed view of a main system component, which is the link between the backbone of the whole infrastructure, and the appealing view for the end client. The technologies mentioned in the diagram itself illustrate some of the best possible technologies to be used that will ensure that the data is transferred securely through all the other parts of the system.

The technologies specified in the diagram are meant to bring up the easiest usage and implementation of security measures in the system, and the frameworks being involved offer far more possibilities, rather than doing most of the parts manually, hence enhancing the speed of implementation and the speed of the system work, as it additionally boosts the performance of the infrastructure.

# Rights of data subject and lawfulness of processing

In the prior chapters, it was specified that out company has the necessity to process some of the data, as that is obligatory in order to provide the company’s services to the client itself. As a matter of fact, it is also necessary to explain the necessity of processing of the data, as well as specifying the legal grounds that our company bases on, in order to make the processing of the data fair and accountable to the rules regarding the lawfulness of processing. The final goal is to obtain a clear view and specify the legal ground(s) for accessing, reading, and processing the data of the client. Additionally, it is important to mention what are the rights that the client obtains at the same time, as that will preserve the balance between rights and duties.

First of all, we will make sure to denote the lawfulness of processing that the company bases itself on, that including, in first order, the Consent, that we require from the client for processing the data (further on that also in this chapter). Another rule that our processing bases upon, includes the fundamental meaning of the lawfulness of Necessity for performance of a contract, even though our company does not plan to provide contracts signed by both parties (company and client) for the moment being.

As mentioned above, one of our lawfulness that we base upon, is the Consent, as our company has the necessity that involves processing of personal achievements (in school or any other institution), and personal preferences or any additional piece of information that will aid the team to provide the client with a proper analytic and support, as that is the main goal of the company. Our company requires the client to provide consent, which will guarantee the client the rights of the data subject and allow our company to provide the service. In terms of receiving consent, it should be specified, that according to the Art. 8.1 (https://gdpr.algolia.com/gdpr-article-8) of GDPR, if the data subject is younger than 16 years old, then there will be additional needs for the consent to be given by a parent. To provide this, our company will ask for a signed form that is supposed to be handed in by the parent via a virtual platform, or via e-mail. The document signed by the parent will state clearly that our company requires the allowance to process the data in order to provide the services. Additionally, it is important to mention that our company is not going to process any of the special categories of special data, from those mentioned in the Art. 9 (<https://gdpr.algolia.com/gdpr-article-9>) of GDPR. The only data that is used to uniquely identify the person is the Unique Student Identifier, that allows the service provider to get access to the achievements of the data subject. Also, our company does not process any data relating to criminal convictions and offences. By guaranteeing our company consent, the data subject obtains the right to withdraw consent, in case the client is subject to stop the work with our company. Apart from that, the client gathers the right of access, as the client is supposed to know what our company uses the information for, and what is the end result of the analysis, which in this case is represented by the support/help that is going to be provided via the virtual platform. The consent is going to be gathered by the online platform itself, as the client will have to accept the terms and conditions before accessing the service itself.

The other lawfulness of processing that our company bases the processing on, is represented by the Necessity for performance of contract, even though our company does not really provide legitimate contracts in their casual form, where there would be necessary a signature from both of the parties. Hence, in our system, we require consent, which is our form of contractual agreement, as that requires agreement from the client. This lawfulness of processing is also related to the processing of the data mentioned in the paragraph above, as the data that is being processed is essential for the performance of the services of our company. Hence, the processing of the data once again will allow our company to provide the client with the required support that is used by the student. In terms of rights of the data subject, the client will be able to gather the right to rectification, as that will empower the client to understand that our company is transparent and responsive to our customers, and tends to keep the most accurate information, so as to avoid possible collisions, or issues. Another right that the data subject gathers, is the right to erasure, as in the previous chapters, it was specified that “*the data will be retained for an additional time of 2 years after the client finishes working with the company*”, and apart from that, we will allow our users to be erased from our database, which includes any processed records.

# Risk mitigation

For the sake of security of our company’s system, it is essential to make an assessment of what are the possible risks and how to mitigate them, as while managing clients data, and different processing operations, it is crucial to make sure that the data stays intact, and that it is possible to provide confidentiality, integrity, and availability of the data, along with securing the infrastructure from possible threats.

In this document we are going to base ourselves upon the Secure Control Framework, which will embed our documentation with more informative layers of defense, and hence engage us to provide a better overview of the real problems and their severity, via grading the possibility of a problem to occur, as well as a method to mitigate the possible issue.

First, we will denote a few levels that will denote the likelihood of a risk to occur:

* Unlikely – Very low chance to occur.
* Possible – Low chance of it occurring.
* Likely – Will occur almost certainly.
* Certain – Will occur.

The above levels denote how possible is the occurrence of an incident that is specified, based upon multiple factors that include the prior hits for other companies and other data that can be used as a factor to identify the risks and likelihood of those to occur.

Additionally, it is needed to specify the possible levels of impact that may occur to the data, or to the system itself, as that will allow the company to prioritize security measures in order to make the best use of the financial means and ensure client data security.

There are a couple levels of possible impact:

* Negligible – No personal data involved, or risk will not have impact.
* Minor – Short-term, involves small amount of sensitive personal data, minimal disruption in service.
* Moderate – More than a minimal amount of sensitive personal data involved, potential of financial loss, minimal disruption in service delivery, short-term distress.
* Major – Significant amount of sensitive information released outside the organization leading to significant actual or potential detriment.
* Catastrophic – Catastrophic amount of sensitive information released outside the organization leading to proven detriment and high-risk safeguarding concerns. Data subjects may encounter significant or irreversible consequences which they may not overcome.

Now, it is important to mention the most important risks that may occur, and then specify the methods to solve, or minimize their impact upon the system, and hence ensure that the data is intact throughout the system, and does not get into the wrong state, or flaw.

Possible risks:

**Data breach**

Likelihood: Possible

Impact: Major

Description: In case of data breach, most of the personal data is becoming endangered as it may get leaked illegally, due to illegal access. This puts the clients and the company in danger, as it questions the security of the system.

Mitigation: Implement data encryption protocols (which will work both for transmission of data, and storage), enhance access controls (as mentioned in the chapters regarding dataflow, that the data is supposed to be accessed via a secure path, and one way to ensure that is securing the access control to the database itself, and then use further implementations in the code), enhance staff awareness regarding security vulnerabilities, like phishing attacks.

**Data loss**

Likelihood: Possible

Impact: Major

Description: Accidental deletion or corruption of student data might occur as a result of unproper management of the software, or software bugs, or any possible impactful change that may lead to the system misbehavior, and loss of important information overall. It can additionally be a consequence of a data breach.

Mitigation: Implement regular data backups stored in secure, off-site locations (meaning locations that are away from the main backbone of the system). Make usage of cloud-based storage solutions with redundancy features, that ensure data integrity and availability. However, such implementations will mean that the data should be transferred securely, and ensured to specify that the data is also stored somewhere not under the company’s full control.

**Data integrity issues**

Likelihood: Unlikely

Impact: Negligible

Description: It represents situations where the data that is stored, is stored inaccurately, which is usually outdated data, or situations where the data was captured in the wrong way, hence causing confusion regarding the personal data. This can also happen in situations where the client specified the data in the wrong way.

Mitigation: Implement data validation checks to ensure the accuracy and completeness of student information at the point of entry (that is where the company can make use of different layer of the application, specified in the dataflow). Implement mechanisms for students to update their information as needed (that is where the company can implement support for the client, via mailing system or something similar). Regularly audit and reconcile data to identify and correct any integrity issues. This is also a point where the client can make use of the right of rectification.

**Unauthorized access**

Likelihood: Possible

Impact: Catastrophic

Description: It represents situations where an individual, or a threat got improper access to the data and to the infrastructural system of the company, and can damage it in a variety of ways, which can be very destructive for the reputation of the company, and the data that is stored on the systems. It is a different level of breach, which is similar to a data breach, though it may affect more parts of the system, rather than the other one.

Mitigation: Implement access controls, including role-based permissions and two-factor authentication (this once again, refers to the data infrastructure like database security, and development environment of the company). Regularly review and update access permissions to ensure only authorized personnel have access to sensitive data (this relates to the possible servers, and production environment overall, where access control for workers can become one of the most important solutions)

# Cookie statement

## What are cookies?

Cookies are small pieces of text used to store information on web browsers. Cookies are used to store and receive identifiers and other information on computers, phones and other devices. Other technologies, including data that we store on your web browser or device, identifiers associated with your device and other software, are used for similar purposes. In this statement, we are going to refer to all of these technologies as “cookies”.

Our company uses cookies if you have an AlwaysNext2You account and use our app, and other websites and apps that can be related to our company. Cookies enable AlwaysNext2to understand the information that we receive about you, including information about your use of other websites and apps, whether you are registered or logged in.

This statement explains how we use cookies and the choices you have. Except as otherwise stated in this statement, the Privacy Policy of our company will apply to our processing of the data that we collect via cookies.

## Why do we use cookies?

Cookies help us provide, protect and improve AlwaysNext2You company, such as by personalizing content and providing a safer experience. The cookies that we use include first-party cookies, which are primarily used to enhance user experience by remembering user preferences, settings, and login information, and session cookies, are used to track user activities during a browsing session and are essential for certain website functionalities, such as maintaining login sessions. The cookies we use may change over time as we improve and update our system, and we typically use them for:

* Authentication (We use cookies to verify your account and determine when you’re logged in so that we can make it easier for you to access the AlwaysNext2You services)
* Security, site and service integrity (We use cookies to help us keep your account and data safe and secure, also to combat activities that violate our policies)
* Performance (We use cookies to provide you with the best experience possible)
* Analytics and research (We use cookies to better understand how people use AlwaysNext2You so that we can improve them)

## Cookie consent

By using AlwaysNext2You service, you consent to the use of cookies and similar technologies in accordance with this cookie statement. If you do not agree to the use of these cookies, please disable or delete them through your web browser settings or refrain from using the service. Once using our service, you can opt to choose one of the options from the service. You can choose to consent and accept all the cookies, consent only essential ones (being the first-party cookies, as they represent the biggest valuable item for our company), accept all of them (which will enable us to collect the cookies specified in this cookie statement), or refuse all (which will restrict the functions that were specified in this cookie statement).

## Cookie duration

The cookies that are used by our service, have a specific duration that they are stored for, but with different means of time. The session cookies are cookies that are stored for a session (as the name specifies), and mean that those cookies are stored in your browser, for the time that you are using it, and will automatically disappear from your browser once you close it, unless specified otherwise by yourself. The first-party cookies are split into multiple ones, and one of them are those that keep you logged in while you navigate through the pages of our AlwaysNext2You online service and are stored for a period of 365 days. The cookies that are used for performance reasons are stored for a period of 7 days. Cookies responsible for analytics and research are stored for a period of 90 days.

## Cookie handling

You can set your cookie settings depending on your preferences. In order to do that, you can change the settings in your browser, which will take care of most actions for you. Here you will be able to find ways to disable cookies for popular web browsers:

* [Firefox](https://cookie-script.com/knowledge-base/disable-cookies-firefox)
* [Google Chrome](https://support.google.com/accounts/answer/61416?hl=en&co=GENIE.Platform%3DDesktop)
* [Brave](https://support.brave.com/hc/en-us/articles/360050634931-How-Do-I-Manage-Cookies-In-Brave)
* [Opera](https://help.opera.com/en/latest/web-preferences/)

For other browsers, please visit your browser’s FAQ page and search for terms related to “cookies”.

By enabling or disabling the cookies settings in your browser, you give it the instructions how to handle the settings for specific websites that you are navigating to, or only specific websites.

## Legal compliance

It is important to mention that our company complies with the GDRP rules and maintains the best possible features that ensure the user security and privacy of user data. In order to comply with the rules engaged by the European Law and GDPR in general, there might be several changes in the cookie statement that alter the cookies that are being used, their storage duration, or means they are used for.

## Updates to the cookie statement

As mentioned, the cookie statement might be updated in order to comply with the updated rules, or in case of the policy changes of the company itself. In such cases, our company is going to contact our clients via electronic means, so as to let you know what the changes are (in a similar way in case of Terms of Agreement change or Privacy Policy changes) and whether there are any actions you need to do in order to have the good experience of using our service. Additionally, you can check the cookie statement eventually in order to identify any possible changes.

## Contact us

If you have any questions, concerns, or feedback regarding our use of cookies or this cookie statement, please feel free to contact us. We value your privacy and are committed to providing transparent information and addressing any inquiries promptly.

You can reach us via email at [e-mail support](mailto:alwaysnext2you@support.next). Our dedicated team is here to assist you and will strive to respond to your inquiries in a timely manner.

Alternatively, you can reach us by mail at the following address:

AlwaysNext2You

Rijelstraat 5

8200

Belgium

We appreciate your interest in our website and your attention to our privacy practices. Your feedback helps us continually improve our services and ensure compliance with data protection regulations.

# Appendix

1. <https://www.facebook.com/privacy/policies/cookies> - Cookies Policy of Meta company
2. <https://miro.com/app/board/uXjVKWhm1IE=/?share_link_id=488385386601> – Better overview of the diagrams for dataflow
3. <https://gdpr.algolia.com/> - website specifying the articles (rules/GDPR) to comply with.