Authologic

TERMS AND CONDITIONS
FOR THE PROVISION OF THE SERVICE
OF ISSUING ELECTRONIC ATTESTATIONS OF ATTRIBUTES

Trust Service Provider:	Authologic sp. z o.o.
Effective from:	13.07.2026
Version:	1
Related document:	Trust Service Policy for the Non-Qualified Electronic Attestation of Attributes Issuance Service provided by Authologic Sp. z o.o., version 1.0.

Authologic

TABLE OF CONTENTS

Authologic

I. WHO WE ARE AND HOW TO CONTACT US

In this section, you will find basic information about Authologic and how you can contact us in matters relating to the Service

1. The Service is provided by Authologic sp. z o.o. with its registered office in Warsaw, street Złota 59, 00-120 Warsaw, Poland, entered in the register of entrepreneurs of the National Court Register under KRS number 0000851095, NIP 5223186837, share capital: PLN 23,800.00.
2. Authologic is entered in the register of trust service providers maintained by the minister competent for informatisation under number *[to be provided].*
3. In all matters related to the Service, you may contact us:
   3.1. by e-mail: contact@authologic.com;
   3.2. in writing: Authologic sp. z o.o., street Złota 59, 00-120 Warsaw, Poland;
   3.3. by telephone: +48 884 570 570;
   3.4. via a contact form or user panel.
4. The Terms and Conditions are available free of charge before the Agreement is concluded. You can download, save and reproduce them on your device.

II. KEY TERMS

In this section, we explain the key terms used in the Terms and Conditions so that it is easier to understand how the Service works

We use plain explanations to make the Terms and Conditions easy to understand. Where we provide the legal meaning of a term, we base it on official definitions or on the meaning resulting from applicable law. The plain explanation does not limit the meaning arising from mandatory provisions of law.

Term	What this means for you	Legal meaning / notes
AGREEMENT	The agreement between you and Authologic for the provision of the Service, concluded on the terms described in the Terms and Conditions.	The Agreement is concluded electronically at the moment indicated in the Terms and Conditions.
ATTRIBUTE	Specific information about you, your status, characteristic, right or entitlement, e.g. age, address, status, professional qualification or right to use a specific service.	Under eIDAS, “attribute” means a characteristic, quality, right or permission of a natural or legal person or of an object.
ATTRIBUTE SOURCE	A data source that we use to confirm an Attribute, e.g. a document, register, system, database, Wallet or other data provider. Before the Service starts, you will be informed about the relevant Attribute Source or the relevant category of Attribute Source, to the extent applicable to the specific process.	Not every attribute source must be an Authentic Source within the meaning of eIDAS. In the TSP Policy, a similar function is performed by the concept of “Authoritative Source”, understood more broadly than an Authentic Source.
AUTHENTIC SOURCE	A special type of data source that is legally recognized as the primary, undisputable source of truth for information about a person or object.	Under eIDAS, “authentic source” means a repository or system, held under the responsibility of a public-sector body or private entity, which contains and provides

		attributes about a natural or legal person or an object and is considered to be the primary or authentic source of that information in accordance with Union or national law, including administrative practice.
AUTHENTICATION	The process of verifying and confirming that a given person is what it claims to be or confirmation of the origin or integrity of electronic data.	Under eIDAS, "authentication" means an electronic process that enables the electronic identification of a natural or legal person to be confirmed, or the origin and integrity of data in electronic form to be confirmed.
AUTHOLOGIC / WE / US	The provider of the Service, i.e. the company with which you enter into the Agreement.	Authologic sp. z o.o. with its registered office in Warsaw. Full company details are provided in point 1 of the Terms and Conditions.
DIGITAL SERVICE	A service that allows data to be processed in a digital form, access to such data, or another interaction with data in digital form.	For the purposes of consumer law, a Digital Service is a service that allows the Consumer to: 1. create, process, store or access data in digital form; 2. share data in digital form uploaded or created by the Consumer or other users of that service; or 3. otherwise interact by means of data in digital form. The Service, including Digital Service, may also be provided by electronic means. This means that the Service is performed remotely, without the simultaneous physical presence of the parties, at the individual request of the User, by transmitting and receiving data through electronic processing and storage devices via a telecommunications network.
DURABLE MEDIUM	For example, e-mail, a paper document or a PDF file.	A material or tool enabling a consumer or trader to store information addressed personally to them in a way that allows access to the information in the future for a period appropriate to the purposes of the information and that permits unchanged reproduction of the stored information.
EAA	Electronic attestation that enables the Authentication of Attributes. An electronic confirmation relies on a specific Attribute that has been attested as part of the Service. An EAA confirms only the Attribute and only to the extent resulting from the content of the given EAA.	Under eIDAS, "electronic attestation of attributes" means an attestation in electronic form that allows attributes to be authenticated.

EAA DATA	Data and information related to the issuance of an EAA concerning you. This may include, in particular, data needed to issue the EAA, information about the Attribute, the Attribute Source, the issuance, non-issuance, making available to you or to your Wallet / EDIW, status, revocation or validity of the EAA, and evidence related to the performance of the Service.	"EAA Data" is a term used in these Terms and Conditions. eIDAS does not contain a separate definition of "EAA Data", but it provides for specific rules concerning personal data related to the provision of EAA services. Such data is logically separated from other data and is not combined with data from other Authologic Services or services of Authologic's commercial partners, in accordance with the rules arising from eIDAS, the TSP Policy and the Privacy Policy.
EAA POLICY / EAAP	A set of rules for a specific type of EAA or a specific use case, e.g. which Attributes are attested, on the basis of which Attribute Sources, in what format and with what validity period.	In the TSP Policy, EAAP means a policy defining rules for a specific EAA issuance scheme or rulebook.
eIDAS	The EU regulation laying down rules on electronic identification, trust services, the European Digital Identity Wallet and EAA.	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (as amended).
ELECTRONIC IDENTIFICATION	A process in which your identity is confirmed in an electronic environment.	Under eIDAS, "electronic identification" means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural or legal person.
ELECTRONIC IDENTIFICATION MEANS	A tool, document, application, token or other solution containing person identification data and capable of being used for Authentication.	Under eIDAS, it is a material and/or immaterial unit containing person identification data and used for Authentication for an online service or, where appropriate, for an offline service.
EUROPEAN DIGITAL IDENTITY WALLET/ EDIW	An application or other digital solution that allows a user to store, control and present person identification data and EAA, for example to confirm their identity, age or status.	Under eIDAS, it is an electronic identification means that allows the user to securely store, validate and manage person identification data and EAA for the purpose of providing them to relying parties and other wallet users, and also allows the creation of qualified electronic signatures or qualified electronic seals.
NON-QUALIFIED TRUST SERVICE PROVIDER	A natural person or a business entity that engages in the provision of non-qualified trust services within the meaning of the eIDAS Regulation.	In this version of the Terms and Conditions, Authologic acts as a non-qualified Trust Service Provider.
QUALIFIED EAA	A special type of EAA that may be issued only by a qualified trust service	Under eIDAS, "qualified electronic attestation of attributes" means an EAA issued by a qualified trust service provider

	provider and must meet additional legal requirements.	and meeting the requirements laid down in Annex V to eIDAS. Under these Terms and Conditions, Authologic provides a non-qualified EAA issuance service. The Service does not include the issuance of Qualified EAAs.
RELYING PARTY	An entity that may rely on the EAA if the EAA is presented to it, for example by you or through your Wallet, and that needs confirmation of a given Attribute.	Under eIDAS, "relying party" means a natural or legal person that relies upon electronic identification, European Digital Identity Wallets, other Electronic Identification Means, or a Trust Service.
SERVICE	The service of issuing an EAA in accordance with the Terms and Conditions and applicable EAAP. The Service relates to an Attribute concerning you or the object to which you hold appropriate rights.	The Service is a non-qualified Trust Service in the field of issuing EAA, provided in accordance with eIDAS, the TSP Policy, the relevant EAA Policy / EAAP and the Terms and Conditions.
SUBSCRIBER	A person or entity that has a separate agreement with Authologic and accepts specific obligations connected with the issuance of an EAA. In the basic consumer model, you use the Service in your own name and the EAA relates to your Attribute.	Subscriber is not a core eIDAS definition. In ETSI standards, it means a natural or legal person bound by agreement with a trust service provider, or with an EAA service provider, to subscriber obligations. A Subscriber is not automatically the same as a Relying Party. The same entity may perform both roles only if this follows from the specific use case and contractual model.
SYSTEM	Our website, application, API, form, widget, link, panel, module or other online tool through which we provide the Service.	Channels for providing the Service, e.g. website, widget, API, application, panel.
TERMS AND CONDITIONS	This document.	The Terms and Conditions define the rules for using the Service and constitute the terms and conditions for the provision of the Service.
TRUST SERVICE	An electronic service that, depending on the type of the service, increases the certainty, security, integrity and authenticity of certain digital activities.	eIDAS defines a catalogue of trust services. The issuance of EAA falls within the scope of eIDAS.
TRUST SERVICE PROVIDER	An entity that provides one or more Trust Services.	Under eIDAS, "trust service provider" means a natural or legal person who provides one or more Trust Services either as a qualified or as a non-qualified trust service provider.
TSP POLICY	A public Authologic document describing the rules, measures and framework for providing the non-qualified Trust Service of issuing EAA.	The draft TSP Policy is "Trust Service Policy for the Non-Qualified Electronic Attestation of Attributes Issuance Service provided by Authologic sp. z o.o.". The TSP

		Policy describes, among other things, the EAA lifecycle, its status, revocation rules, security rules, evidence retention and operational rules.
WALLET	An application or other digital solution in which you can receive, store or present EAA, if the given version of the Service supports that mode of operation.	For the purposes of these Terms and Conditions, "Wallet" is a general term and may include both the European Digital Identity Wallet / EDIW and other wallet-type applications or digital solutions, depending on the specific process. Where the European Digital Identity Wallet / EDIW is concerned, the rules resulting from eIDAS apply.
YOU / CONSUMER / USER	A natural person using the Service as a private person and the person to whom the Attribute and EAA relate.	A consumer is a natural person who enters into the Agreement or uses the Service for purposes not directly related to their business or professional activity. By accepting these Terms and Conditions, it is assumed that you are acting in the capacity of a Consumer.

If we use technical or legal terms in the Terms and Conditions in a simplified way, we do so only to make the Terms and Conditions easier to understand. Such simplifications do not change the meaning of those terms resulting from mandatory provisions of law.

III. WHAT THE SERVICE IS ABOUT

In this section, we describe what the Service is, what roles are involved in the process and what the issuance of an EAA may include

5. The Service consists in issuing an EAA, i.e. an electronic attestation of one or more Attributes.
6. There are two direct roles in the Service model:
   6.1. you — acting as the Consumer and the person to whom the Attribute and EAA relate;
   6.2. Authologic — as the non-qualified Trust Service Provider issuing the EAA.
7. A Relying Party is not a direct participant in the Service covered by these Terms and Conditions. A Relying Party may later rely on the EAA if the EAA is presented to it by you, through your Wallet / EDIW or in another way outside the Service described in these Terms and Conditions. A Relying Party does not become a party to the Agreement between you and Authologic only because it may rely on the EAA. If Authologic has a separate agreement with a business customer, Subscriber or another entity in relation to a specific use case, this does not change your rights under these Terms and Conditions.
8. In practice, the Service may include the following activities:
   8.1. we receive a request to issue an EAA;
   8.2. we collect the data needed to confirm the Attribute;
   8.3. we verify the Attribute in the Attribute Source, if required in the given use case;
   8.4. we issue the EAA in electronic form in accordance with the relevant EAA Policy / EAAP;

8.5. we make the EAA available to you, to your Wallet / EDIW or in another form supported by the specific issuance process, in accordance with the method of operation of the Service and the information shown before the Service starts. Any later presentation, release or use of the EAA in relation to a Relying Party is outside the Service described in these Terms and Conditions. If Authologic provides any separate service related to presentation or release of an EAA, it will be governed by separate terms or the relevant EAA Policy / EAAP.

9. Before a specific Service starts, we will show you at least:
   9.1. which Attribute is to be attested;
   9.2. the Attribute Source or category of Attribute Source, if relevant and applicable to the specific process;
   9.3. the format in which the EAA will be issued e.g. to the Wallet, EDIW or to the electronic document (such as PDF or another format);
   9.4. the EAA's validity period;
   9.5. information that Authologic does not charge you any fee for the Service;
   9.6. the most important limitations and technical requirements.
10. The Service is a non-qualified Trust Service within the meaning of eIDAS to the extent that it consists in issuing EAA. In addition, the Service is not a financial service, payment service, open banking service, credit, insurance, investment or banking service. Authologic does not make financial, credit, AML/KYC or sector-specific decisions on behalf of the Relying Party.
11. The Service is provided in accordance with the Terms and Conditions, the TSP Policy and the relevant EAA Policy / EAAP, if such EAA Policy / EAAP has been adopted for the given use case.
12. The Terms and Conditions define your rights and obligations as a Consumer.
13. The TSP Policy and the EAA Policy / EAAP mainly define technical, operational, security and EAA lifecycle rules. If there is any inconsistency between these documents concerning your consumer rights, the Terms and Conditions and mandatory provisions of law prevail. If the inconsistency concerns the technical interpretation of the EAA, EAA status, EAA format or EAA verification rules, the TSP Policy or the relevant EAA Policy / EAAP apply, provided that this does not limit your rights as a Consumer.

IV. WHAT THE SERVICE DOES NOT INCLUDE

In this section, we explain what the Service is not and which decisions or obligations Authologic does not assume on behalf of other entities

14. The Service is not a Qualified EAA or any other qualified Trust Service.
15. The Service does not replace the Relying Party's decision. The Relying Party independently assesses whether the EAA is sufficient for the purpose for which it is used, unless the law or separate binding arrangements provide otherwise.
16. The Service does not mean that Authologic performs AML/KYC obligations, executes customer due diligence measures, performs regulated onboarding obligations or other sector-specific obligations on behalf of the Relying Party.
17. Authologic does not guarantee that the Relying Party will accept the EAA for certain purposes. An EAA confirms an Attribute only within the scope and on the terms indicated in the EAA and in the information shown before the Service starts.
18. An EAA may not be denied legal effect or admissibility as evidence solely because it is in electronic form or because it does not meet the requirements for a Qualified EAA.
19. We do not automatically update an EAA after it has been successfully issued.

V. WHO THE SERVICE IS FOR

In this section, we indicate who may use the Service and when we may refuse or interrupt its performance

20. The Service is intended for Consumers.
21. For the purposes of this version of the Terms and Conditions, we assume that the Service may be used only by adults, unless the description of a specific Service or the EAA Policy / EAAP states otherwise.
22. We may refuse to provide the Service or interrupt its performance if we have a justified suspicion of abuse, impersonation of another person, use of another person's data, violation of law, including sanctions regulations or the risk of circumvention of such regulations, violation of the Terms and Conditions, a threat to the security of the System or failure to meet the requirements of the relevant EAA Policy / EAAP.
23. Annex 3 to the Terms and Conditions lists your most important rights as a Consumer.

VI. TECHNICAL REQUIREMENTS AND SECURITY RULES

In this section, we describe what you need to use the Service and which basic security rules you should follow

24. To use the Service, you need at least:
    24.1. a device with internet access, e.g. a telephone, tablet or computer;
    24.2. an up-to-date web browser or application supported by the System;
    24.3. an active e-mail address;
    24.4. the ability to receive messages, codes or authorisation links, if required;
    24.5. access to a document, Wallet, EDIW, account or other source of data if needed to issue the EAA;
25. You must not provide through the System any unlawful, false, misleading content, content that infringes the rights of others, or content intended to circumvent the security of the System. Authologic reserves the right to suspend or terminate access to the Service in the event that any breach of these obligations is detected.
26. You must remain diligent and take due care to secure your device, Wallet, passwords, codes, and e-mail access. If you suspect that your device, Wallet, e-mail, or data has been compromised, you must inform us immediately if this could affect the Service or the EAA. If you breach these obligations or contribute to their breach, Authologic's liability shall be excluded or limited to the corresponding extent.
27. When you use the System, we store certain data and similar technologies on your device (e.g. in your telephone or computer memory). We use these technologies to operate the System, ensure security, authenticate and authorise activities, maintain the session, prevent abuse and remember the progress of the process.
28. The technologies we use are divided into two clear categories:
    28.1. strictly necessary technologies (security and operation) - they are necessary to launch the System, maintain your session, secure the process, prevent abuse, authenticate you and perform the Service you requested;
    28.2. analytical and functional technologies (optional) - they help us measure statistics, examine the operation of the System and improve the process. We use them only when the law allows it, including after obtaining your consent, if it is required.
29. A detailed list of these tools, the period for which they are stored on your device and the rules for managing consents can be found in the Cookies Policy.
30. Specific risks related to using the Service and information about the function and purpose of software or data introduced into your device or system are described in Annex 2 to the Terms and Conditions.

VII. INFORMATION BEFORE STARTING THE SERVICE

In this section, we indicate what information we will show you before a specific Service starts

31. Before the Agreement is concluded, we will show you the most important information about the Service in a clear manner, in particular:
    31.1. the main features of the Service;
    31.2. the Attribute to be attested;
    31.3. where and how the EAA will be made available as part of the Service;
    31.4. information that the Service is free of charge for you;
    31.5. the method of performance of the Service and the expected time of performance of the Service;
    31.6. information about functionality, compatibility, interoperability and relevant technical protection measures, if applicable;
    31.7. where applicable, information about your rights after withdrawal from the Agreement in relation to content other than personal data that you provided or created when using the Digital Service;
    31.8. duration of the Agreement,
    31.9. information about the right of withdrawal from the Agreement and the practical consequences of withdrawal if the EAA has already been issued;
    31.10. links to the Terms and Conditions, Privacy Policy, Cookies Policy and - where applicable - TSP Policy or EAA Policy / EAAP.
    31.11. the minimum duration of your obligations under the Agreement,
    31.12. complaint rules and Service provider contact details,
    31.13. the possibility of resorting to out-of-court complaint and redress mechanisms and the rules of access to these procedures.
32. Before a specific Service starts, we will also show you a short summary of the given use case, if this is necessary for you to make an informed decision to use the Service.

VIII. CONCLUSION OF THE AGREEMENT AND CONFIRMATION OF ITS CONCLUSION

In this section, we explain when you enter into an Agreement with Authologic and what confirmation you will receive after it is concluded

33. The Agreement is concluded online.
34. The Agreement is concluded when you perform all activities required in the System, in particular:
    34.1. you read and accept the Terms and Conditions;
    34.2. you confirm that you want to use the Service;
    34.3. we are in possession of your e-mail address.
35. After the Agreement is concluded, we will provide you with confirmation of its conclusion on a Durable Medium or in another way enabling you to save and reproduce the content of the confirmation. The confirmation includes information required by law, including information about the Service, the fact that the Service is free of charge for you, the right of withdrawal and statements made in the System.
36. This Agreement is concluded in English. Communication with us takes place in English, unless we expressly make another language available in a given process. If we make another language version available, we will indicate which version prevails.

IX. SERVICE FLOW STEP BY STEP

In this section, we show a simplified flow of the process - from starting the Service to the issuance or non-issuance of an EAA

37. Our Service is provided according to the following steps:
    37.1. you start a process in which an EAA is needed;
    37.2. we show you the description of the Service, the Attribute, the method of making the EAA available, information that Authologic does not charge you any fee for the Service and the limitations of the EAA;
    37.3. you accept the Terms and Conditions and confirm that you want to use the Service;
    37.4. we issue the EAA or inform you that the EAA cannot be issued;
    37.5. we make the EAA available to you, to your Wallet / EDIW or in another form supported by the specific issuance process, as shown to you before the Service starts.
38. If we cannot issue an EAA, we will inform you of this in an understandable way, unless we are prevented from doing so by law, the security of the System, protection of other persons or anti-abuse rules.
39. Examples of reasons for non-issuance of an EAA include:
    39.1. inability to confirm the Attribute in the Attribute Source;
    39.2. data discrepancy;
    39.3. lack of required authorisation;
    39.4. suspected use of another person's, false or outdated data;
    39.5. unavailability of an external Attribute Source;
    39.6. failure to meet the requirements of the relevant EAA Policy / EAAP;
    39.7. a legal, security or regulatory compliance requirement.
40. If non-issuance of the EAA results from a reason attributable to us, you may submit a complaint in accordance with the Terms and Conditions. If non-issuance of the EAA results from a reason independent of us, e.g. lack of access to the Attribute Source, we will inform you about possible next steps.

X. CONTENT, VALIDITY, STATUS AND REVOCATION OF EAA

In this section, we describe what an EAA may contain, how long it may be valid, how its status can be checked and when it may be revoked

41. The EAA will contain information needed to identify the EAA, Authologic as issuer, the attested Attribute, the scope of attestation and - where applicable - the relevant EAA Policy / EAAP.
42. The detailed EAA format depends on the given use case, the TSP Policy, the EAA Policy / EAAP and applicable technical standards.
43. The validity period of the single use EAA is calculated in minutes, months or years within the timeframe of 15 minutes up to 3 years, in accordance with the information in the EAA and the EAA Policy / EAAP. Authologic reserves the right to shorten or extend expiration dates as needed.
44. Authologic makes available an EAA status list on its official website: www.authologic.com/trustservices. The status indicates, in particular, whether the EAA is revoked or valid.
45. A Relying Party that decides to rely on an EAA is responsible for checking the integrity, authenticity, status, validity conditions and limitations of the EAA. This does not limit Authologic's obligations as the issuer of the EAA to the extent required by law, the TSP Policy or the relevant EAA Policy / EAAP.

46. We may revoke an EAA if required by law, security, a detected error, abuse, expiry of the Attribute, a request by an authorised entity or another important reason related to security, compliance, correctness of the EAA or protection against abuse, as described in the TSP Policy or the relevant EAA Policy / EAAP.
47. You may submit a request to revoke an EAA if the EAA concerns you and you have grounds to do so, e.g. if the EAA contains an error, was issued on the basis of outdated data, the legal or factual status concerning the Attribute has changed, or you suspect abuse. You may submit the request through the communication channels indicated in point 3 of the Terms and Conditions.
48. If you have lost access to the Wallet or EDIW, you may request revocation of the relevant EAA. We will handle such request in accordance with the TSP Policy, the relevant EAA Policy / EAAP and applicable law.
49. After receiving a request to revoke an EAA, we will confirm receipt to the e-mail address or via another channel of contact with you used in the System (if applicable). We may ask you for additional confirmation of identity or control over the Wallet if this is necessary to handle the request securely. We will handle the request without undue delay, no later than within 14 days.
50. If the EAA is revoked, the revocation is irreversible. Obtaining the EAA again requires submitting a new request and re-verification of the Attribute.
51. The Terms and Conditions do not establish a guaranteed minimum availability level for the service or a separate SLA for the Consumer. This does not apply to obligations that cannot be excluded under the law, including consumer rights.

XI. RULES FOR USING EAA

In this section, we explain how the EAA should be used and what you must not do with the issued attestation

52. You may use the EAA only in accordance with its scope, validity period and limitations shown before the Service starts.
53. You must not modify the content of the issued EAA, remove security features, present an EAA after it has been revoked, present an EAA after its validity period has expired or use the EAA in a manner suggesting that it confirms more than results from its content.
54. If you know or should be aware that the Attribute confirmed in the EAA is no longer up to date, you should refrain from using the EAA in a manner that may be misleading. In such a case, you may contact Authologic to clarify whether it is possible to revoke, re-issue or update the EAA.
55. The Relying Party independently assesses whether the EAA is sufficient for the purpose for which it is to be used, unless the law or separate binding arrangements provide otherwise. Authologic does not guarantee that an EAA will be sufficient for any specific purpose of a Relying Party, Subscriber or another third party.

XII. INTELLECTUAL PROPERTY AND RULES FOR USING THE SYSTEM

In this section, we describe the rules for using the System, documentation, Authologic markings and technical solutions used in the Service

56. Rights to the System, its elements, interface, software, documentation, names, trademarks, logo, materials and content made available by Authologic belong to Authologic or to entities whose rights we use lawfully.
57. By using the Service Authologic does not transfer to you any intellectual property rights to the System, software, documentation, Authologic markings or technical solutions used to issue EAA.

58. You may use the System and EAA only to the extent necessary to use the Service and, where applicable, present the EAA in accordance with the Terms and Conditions, the TSP Policy, the relevant EAA Policy / EAAP and the information shown before the Service starts.
59. You must not copy, modify, decompile, analyse source code, circumvent security measures, test the resilience of the System without our consent, remove Authologic markings, modify EAA, falsify EAA or use the System or EAA in a manner that violates the law, the rights of others or the security of the Service.
60. The provisions of this part do not limit your right to use the EAA in accordance with its purpose or your rights resulting from mandatory provisions of law.

XIII. EXTERNAL SERVICES AND SOLUTIONS

In this section, we explain when we may use external solutions and external providers

61. To perform the Service, we may use external solutions or external providers, e.g. Attribute Sources, Wallets, EDIW, ICT providers, security services, anti-abuse tools, technical infrastructure and technical service providers. If using a given external solution requires accepting separate terms or reading separate information, it will be shown to you before such a solution is used, to the extent it concerns your process.
62. We are not responsible for the terms, privacy policies, availability or operation of external solutions to the extent that they are provided by independent entities (e.g. the operator of your Wallet / EDIW or the website, application or service of an independent third party through whose process you access the Service) as they are beyond our control. The above does not exclude our liability for entities with the help of which we perform the Service, nor our liability for proper performance of the Service to the extent we are responsible for it under the law.

XIV. FREE SERVICE

In this section, we explain that the Service is free of charge for you and that no payment is required from you for using the Service

63. Authologic does not charge you any fee for the Service. Another entity may charge you for its own services, products or process independently of Authologic. Such fees are not charged by Authologic and are not governed by these Terms and Conditions.
64. Before the Service starts, we will show you information that the Service is free of charge for you.
65. The Service may be financed by another entity, business customer or provided in another business model. This does not create any payment obligation for you towards Authologic.
66. The fact that the Service is free of charge for you does not mean that you consent to the use of EAA Data for purposes unrelated to the Service, e.g. for marketing, profiling or creating user profiles outside the Service.
67. If you receive a request for payment allegedly on behalf of Authologic in connection with the Service, do not make the payment and contact us using the channels indicated in point 3 of the Terms and Conditions.

XV. START AND PERFORMANCE OF THE SERVICE

In this section, we explain when we start performing the Service and what may affect the time of its performance

68. The Service is intended to be performed immediately after the Agreement is concluded, unless the information shown before the Service starts, the TSP Policy or the relevant EAA Policy / EAAP provides otherwise.

69. This means that the EAA is to be issued shortly after the Agreement is concluded, provided that the requirements for issuing the EAA are met.
70. The actual performance time may depend on your actions, availability of the Attribute Source, Wallet / EDIW, technical availability of the System or additional security verification.
71. If performance of the Service cannot be completed, we will inform you about this in an understandable way, unless we are prevented from doing so by law, security of the System, protection of other persons or anti-abuse rules.

XVI. RIGHT OF WITHDRAWAL FROM THE AGREEMENT

In this section, we describe when you may withdraw from the Agreement and what withdrawal means if the EAA has already been issued

72. If you enter into the Agreement as a Consumer, as a rule you may withdraw from the Agreement within 14 days from the date of its conclusion without giving any reason.
73. To withdraw from the Agreement, inform us of your decision by contacting us in the manner indicated in point 3.4. of the Terms and Conditions. You may use the form in Annex 1, but this is not mandatory.
74. To meet the deadline, it is sufficient to send the withdrawal statement before the expiry of 14 days.
75. The Service is intended to be performed immediately after the Agreement is concluded.
76. If you effectively withdraw from the Agreement before the EAA has been issued, we will not issue the EAA or will interrupt the issuance process, if technically possible.
77. If the EAA has already been issued before withdrawal, withdrawal from the Agreement does not automatically revoke the EAA. The status and revocation of the EAA will be handled in accordance with the Terms and Conditions, the TSP Policy, the relevant EAA Policy / EAAP and applicable law.
78. Because the Service is free of charge for you, withdrawal from the Agreement does not create any financial settlement obligation between you and Authologic.
79. If the law requires a function for withdrawal from an Agreement concluded through an online interface, we will make such function available in the System for the period during which you have the right to withdraw from the Agreement. The function will be labelled clearly, e.g. “withdraw from the contract here”, and will allow you to submit and confirm the withdrawal statement. After you submit the statement, we will send you confirmation of receipt on a Durable Medium.
80. After effective withdrawal from the Agreement, to the extent required by consumer law, we will not use content other than personal data that you provided or created when using the Digital Service, except where the law allows us to continue using such content. At your request, and to the extent required by consumer law, we will make available to you, at our expense, within a reasonable time and in a commonly used machine-readable format, content other than personal data that you provided or created when using the Digital Service. This does not apply to personal data. Information about personal data, including EAA Data, is provided in the Privacy Policy.

XVII. COMPLAINTS, STATUTORY CONSUMER RIGHTS. REPORTING ERRORS, FRAUD AND INCIDENTS

In this section, we explain how you can file a complaint, report an error, abuse or incident, and what rights you have as a Consumer

81. You have the right to file a complaint if you believe that the Service was performed incorrectly, the EAA contains an error, a technical problem occurred which has an impact on the Service or you have other concerns regarding the Service.
82. You may file a complaint using the options indicated in point 3 of the Terms and Conditions.
83. In your complaint, please provide full name, the e-mail address used in the Service, a description of the problem, the date of using the Service, the case or EAA identifier and what you expect. If you do not provide an e-mail address and we have not collected it during the process of providing the Services, we may not be able to contact you.
84. We will respond to the complaint on a Durable Medium within 14 days from the date of receipt. If the law provides that failure to respond within that period means that the complaint is accepted, we will apply those provisions.
85. The Terms and Conditions do not limit your statutory rights as a Consumer. If the Service is not in conformity with the Agreement, you may exercise the rights provided for in applicable consumer rights regulations, in particular request that the Service be brought into conformity with the Agreement or withdraw from the Agreement — in the cases and on the terms provided for in those regulations.
86. If the problem consists in an error in the EAA and the error is on our side, we will take appropriate action, e.g. re-issue the EAA, revoke the erroneous EAA, correct the error or apply another measure that is lawful, proportionate and technically possible in the given case.
87. If the problem results from data originated in an external Attribute Source, we may explain to you what the problem is, but we may not always be able to change data in such a source ourselves. In such a case, it may be necessary to contact the entity maintaining the Attribute Source.
88. If you notice an error in the EAA, suspect unauthorised use of your data, loss of control over the Wallet or EDIW, an attempt to impersonate you, or other abuse related to the Service, report it immediately in the manner specified in point 3 of the Terms and Conditions. Such a report may be handled independently of a complaint if it requires rapid security action, e.g. checking the EAA status, temporarily limiting the use of the EAA, revoking the EAA or securing the process. If the report also concerns incorrect performance of the Service, you may also file a complaint in accordance with the Terms and Conditions.
89. To the extent that the Service constitutes a Digital Service or includes the supply of digital content within the meaning of the Act on Consumer Rights, we are responsible for the conformity of the Service with the Agreement on the terms provided for in that act.
90. The Service should comply with the description, functionality, compatibility, interoperability, technical protection measures, security, technical support and other features agreed with you or resulting from the law.
91. We do not provide automatic updates of an EAA after it has been issued, unless the description of the specific EAA, the TSP Policy, the EAA Policy / EAAP or mandatory provisions of law provide otherwise.
92. We record information needed to demonstrate performance of the Service, in particular the date and time of conclusion of the Agreement, submitted confirmations, requests or statements, if any, the status of performance of the Service and information about issuance, non-issuance, making available or revocation of the EAA. Details of retention and legal bases for processing are described in the Privacy Policy.

XVIII. OPERATION OF THE SYSTEM AND TECHNICAL BREAKS

In this section, we describe when the System may be temporarily unavailable and when we may restrict access to the Service for security or technical reasons

93. We make efforts to ensure that the System operates in a stable and secure manner. However, the Service may be temporarily unavailable, in particular due to technical work, updates, failures, security activities or unavailability of external providers or Attribute Sources.
94. We will inform you about planned material technical breaks in advance, if possible.
95. We may temporarily restrict access to the Service if this is necessary for the security of the System, data protection, prevention of abuse, performance of a legal obligation or ensuring proper operation of the Service.

XIX. LIABILITY

In this section, we explain what Authologic is responsible for and in which situations liability may be limited in accordance with the law

96. We are responsible for performing the Service in accordance with the Agreement, the Terms and Conditions, the TSP Policy, the relevant EAA Policy / EAAP and the mandatory provisions of law.
97. No provision of the Terms and Conditions excludes or limits our liability towards the Consumer to the extent this would be prohibited by law.
98. To the extent permitted by mandatory provisions of law, we are not responsible for consequences resulting from:
    98.1. your providing false, another person's, fraudulent or outdated data;
    98.2. lack of access to your device, e-mail, Wallet, EDIW, or Attribute Source, if this is not due to our fault;
    98.3. a decision of the Relying Party, which independently assesses whether and for what purpose it accepts the EAA, unless the law or a separate agreement provides otherwise;
    98.4. irregularities in data in an external Attribute Source over which we have no control, unless we are responsible for this under the law;
    98.5. use of the EAA contrary to its scope, limitations, validity period or EAA Policy / EAAP;
    98.6. force majeure or external events that could not have been foreseen or avoided despite due diligence,
    98.7. revocation of an EAA by the Authentic Source or by the Subscriber, where applicable and in accordance with the TSP Policy or the relevant EAA Policy / EAAP.
99. For the purposes of point above, force majeure means an external event independent of the party invoking it, impossible to foresee with due diligence and impossible to avoid or overcome, which prevents or materially hinders the performance of obligations under the Terms and Conditions or the Agreement. Force majeure may include, in particular: natural disasters, fire, flood, earthquake, epidemic, acts of war, terrorist acts, riots, general strikes, failures of public infrastructure, long-term interruptions in electricity or internet supply, a cyberattack of a scale and nature impossible to repel despite appropriate security measures, and acts of public authorities preventing the performance of the Service.
100. Where we are not liable in accordance with the above cases, this does not limit your rights arising from complaints, non-conformity of the Service with the Agreement or other mandatory provisions protecting the Consumer.

XX. PERSONAL DATA, EAA DATA AND COOKIES

In this section, we indicate where you can find information on the processing of personal data, cookies and similar technologies

101. We process personal data in connection with the Service. Detailed information on data processing rules can be found in the Privacy Policy: https://authologic.com/pl/privacy-policy

Authologic

102. Information about cookies and similar technologies can be found in the Cookies Policy: https://authologic.com/pl/cookies-policy
103. Personal data related to the provision of the EAA Service is logically separated from data processed as part of other Authologic services or services of our commercial partners. We do not combine EAA Data with data from other Authologic services or services of commercial partners, and we do not use such data for tracking, profiling, behavioural correlation or marketing. This does not apply to processing that is strictly necessary within the EAA Service itself, including the issuance of an EAA, handling of EAA status, security, complaints, fraud prevention or compliance with a legal obligation, in accordance with the Privacy Policy.
104. After issuing an EAA, we do not track where or how you use it. This does not apply where you use functions made available by Authologic as part of the EAA Service, such as checking the status of an EAA, handling a complaint, reporting an error, abuse or security incident, or where processing is required by law.
105. If we use automated analysis, liveness checks, document analysis, biometrics or anti-abuse tools in the Service, we inform about this in the Privacy Policy and in the System to the extent required by law.
106. We do not use EAA Data for purposes unrelated to the Service; in particular, we do not use EAA Data for marketing, enriching user profiles, tracking you across different services or profiling that is not necessary to perform the Service.

XXI. AMENDMENTS TO THE TERMS AND CONDITIONS

In this section, we describe when we may amend the Terms and Conditions, how we will inform you and what rights you have in connection with an amendment

107. We may amend the Terms and Conditions only for important reasons.
108. An important reason may be:
    108.1. a change in laws, guidelines, decisions or positions of authorities affecting the Service;
    108.2. a change in requirements relating to Trust Services, EAA, security and cybersecurity, accessibility, ICT services or consumer protection;
    108.3. a change in the operation of the Service, System, Wallet, EDIW, Attribute Sources, TSP Policy, EAA Policy / EAAP or technical standards;
    108.4. introduction of new features or change of existing features, provided this does not infringe acquired rights of the Consumer;
    108.5. the need to remove errors, ambiguities or gaps in the Terms and Conditions;
    108.6. a change in contact details, registration data, names, links or communication channels;
    108.7. the need to prevent abuse, fraud, security breaches or unlawful activities.
109. We will publish the new version of the Terms and Conditions on our official website. If you have an ongoing relationship with us or we know your e-mail address, we will inform you about the amendment at least 14 days before it enters into force, unless earlier entry into force is necessary due to law, security, an authority decision, an incident or the prevention of abuse.
110. An amendment to the Terms and Conditions does not affect one-off Services, by which we understand the Services that have already been fully performed before the amendment enters into force.
111. We keep information about the version of the Terms and Conditions accepted when the Agreement was concluded and, upon request, will provide it to you on a Durable Medium.
112. If an amendment concerns an ongoing contractual relationship, you may terminate the Agreement before the amendment enters into force by contacting us in the manner indicated in point 3 of the Terms and Conditions.

Authologic

113. We will not change material terms of the Agreement concluded with you to your detriment without a legal basis or your explicit consent.
114. The TSP Policy, EAA Policy / EAAP, Privacy Policy and Cookies Policy may be updated according to the rules described in those documents. If a change to those documents affects your material rights or obligations under the Agreement, we will inform you in accordance with the Terms and Conditions or the law. A change to technical or informational documents may not limit your rights as a Consumer resulting from mandatory provisions of law.

XXII. TERMINATION OF USE OF THE SERVICE

In this section, we explain when use of the Service ends and which obligations may continue after you stop using the Service

115. If the Service is one-off, the Agreement ends after it is performed, unless the Terms and Conditions, the TSP Policy, the EAA Policy / EAAP or the description of the Service provide for additional activities, e.g. complaint handling, checking EAA status, revoking EAA or storing evidence for a specified period.
116. If we make a user account or a continuous Service available, you may resign from further use of the account or such Service at any time by contacting us in the manner indicated in point 3 of the Terms and Conditions or using a function available in the System, if we make it available.
117. Resignation does not affect one-off Services performed before resignation, issued EAA, complaint handling, the possibility of submitting a request to revoke an EAA, storage of evidence of performance of the Service or obligations which, under the law, the Terms and Conditions, the TSP Policy or the relevant EAA Policy / EAAP, should continue after termination of use of the account or continuous Service.
118. We may suspend or terminate access to the Service if you violate the Terms and Conditions, the law, rights of other persons, security rules or use the Service contrary to its purpose. We will apply a measure proportionate to the breach and, if possible and lawful, inform you of the reason.
119. If we terminate provision of the Service, we will apply the termination rules described in the TSP Policy and applicable law, including rules concerning still valid EAA, EAA status, security and storage of evidence.
120. We may send you technical and service messages concerning the Service, e.g. confirmation of conclusion of the Agreement, an authorisation link, one-time code, information about issuance of EAA, non-issuance of EAA, complaint, revocation of EAA, EAA status or security. Such messages are related to performance of the Service, security, process handling or Authologic's legal obligations and do not constitute marketing communication.
121. We conduct marketing communication only when we have an appropriate legal basis.

XXIII. DISPUTES, GOVERNING LAW AND CONSUMER ASSISTANCE

In this section, we indicate which law applies to the Agreement, where you can seek consumer assistance and what options exist for amicable dispute resolution

122. The Agreement is governed by Polish law. This does not deprive you of protection that cannot be excluded under the law of the country of your habitual residence, if such provisions apply.
123. Disputes are resolved by the competent common court. The Terms and Conditions do not limit your right to bring a case before a court competent under consumer protection rules.
124. You may use free assistance from a municipal or district consumer ombudsman, consumer organisations or information available on the website of the Polish Office of Competition and Consumer Protection (UOKiK).

125. If you filed a complaint to us and the complaint was rejected, you can request mediation or an adjudication from a Voivodship Trade Inspectorate arbitration tribunal. For more information, go to the website of the Office of Competition and Consumer Protection (UOKiK) at http://www.uokik.gov.pl/spory_konsumenckie.php.
126. You may also use out-of-court consumer dispute resolution methods if the given dispute qualifies for such procedure and the competent entity conducts it. Information on amicable resolution of consumer disputes is available on the UOKiK website: polubowne.uokik.gov.pl.
127. Authologic does not give a general, standing consent to participate in all ADR proceedings. If, after completion of the complaint procedure, the dispute is not resolved, we will inform you on a Durable Medium whether we agree to participate in a specific ADR proceeding.

XXIV. FINAL PROVISIONS

In this section, you will find rules concerning the availability of the Terms and Conditions, the effects of invalidity of certain provisions and the list of annexes

128. The current version of the Terms and Conditions is available on the official website of Authologic on a Durable Medium - i.e. in a manner enabling it to be downloaded, saved and reproduced.
129. The Terms and Conditions are made available free of charge before the Agreement is concluded and for a period allowing their content to be read, saved and reproduced in the ordinary course of activities.
130. If any provision of the Terms and Conditions is found invalid or ineffective, the remaining provisions remain in force. The relevant provisions of law apply in place of the invalid or ineffective provision.
131. No provision of the Terms and Conditions excludes or limits Consumer rights arising from mandatory provisions of law.
132. If the Service is extended to Users other than consumers, these Terms and Conditions shall apply to them accordingly, with the explicit exclusion of provisions concerning consumer information obligations, procedures for amending the Terms and Conditions, as well as statutory termination and withdrawal rights reserved solely for consumers (especially rights listed in Annex 3).
133. In matters not regulated by the Terms and Conditions, applicable law applies, in particular provisions concerning Trust Services, provision of services by electronic means and Consumer protection, if applicable.
134. Authologic stores archived versions of the Terms and Conditions together with information on their period of validity. At the Consumer’s request, Authologic will provide the Consumer with the version of the Terms and Conditions accepted when concluding their Agreement, on a Durable Medium.
135. To the extent not regulated in these Terms and Conditions, the technical, operational and security rules for the issuance, making available, status, revocation and interpretation of EAAs are specified in the TSP Policy and the applicable EAA Policy / EAAP, provided that this does not limit the Consumer’s rights arising from mandatory provisions of law.
136. The following annexes form an integral part of the Terms and Conditions:
    136.1. Annex 1 - Withdrawal form;
    136.2. Annex 2 - Specific risks related to using the Service and information about technologies used in the System;
    136.3. Annex 3 - Your most important rights as a Consumer.

Authologic

ANNEX 1 TO THE TERMS AND CONDITIONS - WITHDRAWAL FORM

Addressee: Authologic sp. z o.o., street Złota 59, 00-120 Warsaw, Poland.

I, the undersigned, hereby give notice of withdrawal from the Agreement for the provision of the Service of issuing an electronic attestation of attributes (EAA).

Date of conclusion of the Agreement:	
Consumer's full name:	
E-mail address used for the Service:	
Consumer's address, if applicable:	
Date:	
Consumer's signature, if the form is sent on paper:	

Authologic

ANNEX 2 TO THE TERMS AND CONDITIONS - SPECIFIC RISKS RELATED TO USING THE SERVICE AND INFORMATION ABOUT TECHNOLOGIES USED IN THE SYSTEM

I. Purpose of the Annex

1. This Annex describes the specific risks related to using the Service provided electronically and the function and purpose of software or data that Authologic may introduce into the device or system you use.
2. The Annex is intended to help you use the Service safely, in particular because the Service may concern your identity, Attributes, Wallet, EDIW, documents, identification data and EAA.
3. The information in this Annex does not replace the Privacy Policy or the Cookies Policy. Detailed information on personal data processing, cookies and similar technologies can be found in those documents.
4. This Annex does not mean that Authologic provides a service of presenting or releasing the EAA to a Relying Party. Any later presentation or use of the EAA in relation to a Relying Party is outside the Service described in the Terms and Conditions. If Authologic provides any separate service related to presentation or release of an EAA, it will be governed by separate terms or the relevant EAA Policy / EAAP.

II. Key security rules

1. Use the Service only through official websites, applications, links, forms or tools indicated by Authologic or by the entity through whose process you access the Service.
2. Do not provide your data, authorisation codes, passwords, document data, Wallet data or login credentials if you have doubts whether the website, message, link or form really comes from Authologic or from the entity through whose process you access the Service.
3. Do not use the Service on a device that you suspect has been taken over, infected with malware or used by unauthorised persons.
4. Do not disclose to other persons SMS codes, one-time codes, authorisation links, access data to your e-mail, access data to your Wallet, EDIW or data required to issue an EAA.
5. If you suspect abuse, impersonation, loss of control over the Wallet or EDIW, takeover of a device, unauthorised use of your data or an error in the EAA, report this immediately to Authologic using the channel indicated in the Terms and Conditions.

III. Specific risks associated with using the Service

Using the Service may involve, in particular, the following risks:

A. Impersonation of Authologic or another entity involved in the process

1. A third party may attempt to impersonate Authologic, the entity through whose process you access the Service, a Relying Party or another trusted entity, for example through a fake website, fake e-mail, SMS message, messenger, fake QR code or fake link. The purpose of such action may be to obtain your data, documents, authorisation codes, access to the Wallet or EDIW, or to induce you to use or present the EAA in an unsafe way.
2. Before starting the process, check whether you are using the correct link, domain, application or form. If you have any doubts, contact Authologic through the channel indicated in the Terms and Conditions.

B. Fraudulent obtaining of codes, links or authorisations

1. One-time codes, authorisation links, confirmations in the Wallet or EDIW or other authorisation mechanisms may be used to confirm your action in the Service.
2. A third party may attempt to induce you to provide such a code, click a link or approve an operation that you do not understand. Do not approve an operation if you do not recognise the Service, the Attribute, the Wallet / EDIW, the requested action or the effect of that action.

C. Compromise of the device, e-mail account or Wallet (EDIW)

1. If a third-party gains access to your device, e-mail inbox, telephone number, application or Wallet or EDIW, they may attempt to use that access to start the process, confirm the Attribute, receive the EAA or present the EAA.
2. Protect your device with a password, PIN, biometrics or another security mechanism. Keep your operating system, browser and applications up to date.
3. If you suspect that your device, e-mail account, telephone number or Wallet has been compromised, immediately change your access credentials, secure your account and report the problem to Authologic if it may relate to the Service or the EAA.

D. Malware and unsafe extensions

1. Malware, unsafe browser extensions or applications from untrusted sources may intercept data entered in the System, change the content of websites, substitute fake forms or take over the session.
2. Use an up-to-date operating system, an up-to-date browser, legal software and basic device security measures.
3. Avoid installing applications and extensions from unknown sources, especially before starting a process concerning your identity, documents, Attributes or EAA.

E. Use of public or shared devices

1. Using the Service on a public, business, shared or unsecured device may increase the risk of third parties accessing your data, session, documents or EAA.
2. If you use such a device, make sure that after completing the process you have logged out, closed the browser, have not saved login details and have deleted downloaded files if they were saved locally.
3. If possible, use the Service on your own trusted device.

F. Incorrect, third-party or outdated data

1. Providing false, third-party, incomplete or outdated data may result in refusal to issue the EAA, issuance of an incorrect EAA, revocation of the EAA or other consequences provided for in the Terms and Conditions and applicable law.
2. Before confirming the data, check whether it is correct and up to date.
3. Do not attempt to obtain an EAA concerning another person unless you have a clear legal basis to do so (e.g. acting as a proxy) and this follows from a specific process made available by Authologic.

G. Incorrect interpretation of the EAA

1. The EAA confirms only the Attribute indicated in its content, within the scope, validity period and limitations resulting from the EAA, the Terms and Conditions, the TSP Policy, the relevant EAA Policy / EAAP and the information shown before the Service starts.

2. The EAA should not be used after the expiry of its validity period, after revocation, contrary to its limitations or in a way suggesting that it confirms more than results from its content.

H. Use of the EAA after a change of the Attribute

1. The Attribute may change after the EAA has been issued, for example due to a change of status, entitlement, data or information in the Attribute Source.
2. If you know that the Attribute has changed or that the EAA has become outdated, do not use the EAA in a way that may be misleading and contact Authologic if revocation, update or re-issuance of the EAA is necessary.

I. Unavailability of the System, Wallet, EDIW or Attribute Source

1. The Service may depend on the operation of the System, Wallet, EDIW, Attribute Source, communication services, infrastructure providers or other technical tools.
2. Temporary unavailability of any of these elements may result in delay, interruption of the process, inability to issue the EAA or inability to check the status of the EAA.
3. In such a case, Authologic takes actions in accordance with the Terms and Conditions, the TSP Policy, the relevant EAA Policy / EAAP and security and business continuity procedures.

J. Risks related to later presentation of the EAA outside the Service

1. If the EAA is issued to your Wallet / EDIW, you may later present it to another entity through the Wallet / EDIW or in another way supported by the specific process. This later presentation is outside the Service described in the Terms and Conditions. If such later presentation is supported by a separate Authologic service, it will be governed by separate terms or the relevant EAA Policy / EAAP.
2. For your safety, before approving any later presentation of the EAA, check which Wallet / EDIW or other entity is involved and which Attribute is being presented.
3. Do not approve the presentation of the EAA if you do not recognise the requested action, the Attribute or the entity to which the EAA is to be presented.
4. Once the EAA has been issued to you or to your Wallet / EDIW, Authologic does not have control over when, where or to whom you later present the EAA. If such later presentation is supported by a separate Authologic service, it will be governed by separate terms or the relevant EAA Policy / EAAP.

IV. Actions taken by Authologic to reduce risks

1. Authologic applies technical and organisational measures appropriate to the nature of the Service, in particular measures intended to protect the confidentiality, integrity, authenticity, accountability and availability of the Service.
2. Depending on the specific use case, Authologic applies, in particular:
   2.1. encrypted connection;
   2.2. authorisation and Authentication mechanisms;
   2.3. security logs;
   2.4. mechanisms for preventing abuse;
   2.5. verification of data integrity;
   2.6. verification of EAA status;
   2.7. limitation of session validity time;
   2.8. monitoring of security events;

2.9. mechanisms for confirming consents, statements and requests submitted in the System.

3. For security reasons, Authologic does not disclose all technical details of the security measures used, as this could facilitate circumvention of the System or abuse.

V. Function and purpose of software or data introduced into your device or system

1. When using the Service, Authologic may introduce certain data, files, identifiers, scripts, technical components or similar technologies into your device, browser, application or system.
2. Such elements may be used, in particular, for the following purposes:
   2.1. launching and correctly displaying the System;
   2.2. maintaining the user session;
   2.3. remembering the progress of the process;
   2.4. handling authorisation and Authentication;
   2.5. delivering technical messages;
   2.6. ensuring the security of the System;
   2.7. detecting and limiting abuse;
   2.8. confirming the submission of statements, consents or requests;
   2.9. handling technical errors;
   2.10. measuring System performance and technical diagnostics;
   2.11. handling the Wallet or EDIW, if a given process includes the Wallet or EDIW;
   2.12. making the EAA available to you or to your Wallet / EDIW, or enabling the EAA status to be checked, if applicable to a given process.
3. Authologic may use, in particular:
   3.1. cookies necessary for the operation of the System;
   3.2. data in browser storage;
   3.3. session identifiers;
   3.4. technical tokens or authorisation links;
   3.5. scripts necessary for the operation of a form, widget, application or module;
   3.6. technical data concerning the device, browser, operating system, connection time, IP address, language settings, technical errors or security events;
   3.7. mechanisms used to detect abuse, protect against automated attacks, protect against impersonation and protect the integrity of the process.
4. If certain cookies, similar technologies, scripts, analytical tools, marketing tools or other technologies require your consent, we will ask you for such consent in accordance with applicable law.
5. Technologies necessary for the operation of the Service, security, authorisation, session handling, prevention of abuse or performance of the action requested by you may be used to the extent permitted by law without separate consent, provided that they are actually necessary for these purposes.
6. Detailed information about cookies and similar technologies, including their categories, duration and how to manage consents, can be found in the Cookie Policy.

VI. Technical and service messages

1. In connection with the Service, we may send you technical and service messages, for example:
   1.1. confirmation of conclusion of the Agreement;
   1.2. authorisation link;
   1.3. one-time code;
   1.4. information about the start or end of the process;

1.5. information about issuance or non-issuance of the EAA;
1.6. information about a technical error;
1.7. information about a complaint;
1.8. information about revocation, status or validity of the EAA;
1.9. information about security or suspected abuse.

VII. What Authologic will not require from you outside the correct process

1. Authologic will not require you to:
   1.1. provide the password to your e-mail inbox;
   1.2. provide the password to your Wallet or EDIW;
   1.3. provide full login details to external services, unless this follows directly from the secure authorisation process applicable to a given Attribute Source;
   1.4. provide a one-time code to a third party;
   1.5. install an application from an unknown source;
   1.6. disable device security measures;
   1.7. provide the PIN or seed phrase / recovery phrase to your European Digital Identity Wallet or another Wallet-type application.
2. If you receive a request to take such action, exercise caution and contact Authologic through the channel indicated in the Terms and Conditions.

VIII. Reporting threats, errors and abuse

1. Report to us immediately, in accordance with the rules indicated in the Terms and Conditions:
   1.1. suspected impersonation of you;
   1.2. suspected use of your data without consent;
   1.3. compromise or loss of control over the Wallet or EDIW;
   1.4. receipt of a suspicious link, message or code concerning the Service;
   1.5. an error in the EAA;
   1.6. suspected misleading, unauthorised or unsafe use of the EAA;
   1.7. suspicion that the EAA was issued on the basis of false, third-party or outdated data;
   1.8. another event that may affect the security of the Service, your data or the EAA.
2. A report of a threat, error or abuse may be handled independently of a complaint if it requires swift security action.
3. If the report also concerns improper performance of the Service, you may also submit a complaint in accordance with the Terms and Conditions.

IX. Update of information

1. Information about threats, functions and purposes of technologies used in the System may be updated if the Service, System, operation of the Wallet or EDIW, Attribute Source, security threats, applicable law or technical measures used change.
2. The current version of this Appendix is made available in a way that allows it to be downloaded, saved and reproduced.

Authologic

ANNEX 3 TO THE TERMS AND CONDITIONS - YOUR MOST IMPORTANT RIGHTS AS A CONSUMER

This Annex presents, in a simple way, your most important rights related to using the Service. It does not limit the rights you have under the Terms and Conditions or applicable law.

I. You have the right to clear information before the Service starts

Before the Service starts, we will show you the most important information about which Attribute is to be attested, where and how the EAA will be made available as part of the Service, the EAA's validity period, that the Service is free of charge for you and what the most important limitations of the EAA are.

II. You have the right to receive the Terms and Conditions before the Agreement is concluded

We make the Terms and Conditions available free of charge before the Agreement is concluded, in a manner enabling them to be downloaded, saved and reproduced.

III. You have the right to withdraw from the Agreement

If the EAA has already been issued before you withdraw, withdrawal from the Agreement does not automatically revoke the EAA. The status, revocation or invalidation of the EAA is handled according to the Terms and Conditions, the TSP Policy, the relevant EAA Policy / EAAP and applicable law. Because the Service is free of charge for you, withdrawal does not create any financial settlement obligation between you and Authologic.

IV. You have the right to file a complaint

You may file a complaint if you believe that the Service was performed incorrectly, the EAA contains an error, you did not receive the EAA, a technical problem occurred or you have other concerns regarding the Service.

V. You have the right to conformity of the Service with the Agreement

The Service should be performed in accordance with the Terms and Conditions, the information shown before the Service starts, the relevant TSP Policy, the EAA Policy / EAAP and the law. If the Service is not in conformity with the Agreement, you may exercise the rights provided to Consumers under applicable law.

VI. You have the right to report an error, abuse or incident

If you notice an error in the EAA, suspect use of your data without consent, loss of control over the Wallet or EDIW, impersonation of you or other abuse, you may report this to Authologic using the channel indicated in the Terms and Conditions.

VII. You have the right to request revocation of an EAA

You may submit a request to revoke an EAA if the EAA concerns you and you have grounds to do so, e.g. the EAA contains an error, was issued on the basis of outdated data, you suspect abuse or you lost control over the Wallet or EDIW.

VIII. You have the right to protection of personal data

Information about the processing of your personal data can be found in the Privacy Policy.

IX. You have the right to consumer assistance and out-of-court dispute resolution

You may use assistance from a municipal or district consumer ombudsman, consumer organisations or information available on UOKiK websites. You may also use out-of-court consumer dispute resolution methods if the given dispute qualifies for such procedure.