MEMBER ONBOARDING PRIVACY NOTICE

Altura Credit Union Limited

This Data Privacy Notice is effective as and from 11th day of February 2021

Credit Union Contact Details	
Address	Altura Credit Union Limited Mc Dermott Street
	Gorey
	County Wexford
Phone	0539488700
Email	info@alturacu.ie
Website	www.alturacu.ie
Privacy Notices , Cookie Policy and Information on GDPR	The 'About' Section of our website 'GDPR, Altura Credit Union and You' **https://www.alturacu.ie/gdpr-and-you**

Data Protection Officer Contact Details	
Name/Title	Donal O'Connor
Phone	0539488700
Email	dp@alturacu.ie

Introduction

It is important that you are informed before you proceed with this Member Onboarding application. The app provides our members with access to online banking functionality via a mobile app interface. The online member onboarding introduces a functionality that will be openly accessible to anyone who downloads the app, and will not require login. The purpose of this Data Privacy Notice is to explain how Altura Credit Union Limited may process your personal information at the outset of your application for Membership and through the Member Onboarding APP. This Notice also explains how we manage your data following a successful application to become our member however for detailed information on how your data is managed after a successful onboarding application, please see our various other Data Notices on our website addressing different data processing scenarios.

Will someone contact me?

A member of staff within Altura Credit Union may contact the person identified in the onboarding application by phone, text or email in connection with it. In order to process your application, we will share your personal data with third parties who perform important functions for us through the APP . We are also required to cooperate by law with Irish regulatory or enforcement bodies. The details provided by you through the Member Onboarding process together with any other information that is furnished to us in connection with this Member onboarding application will be retained and processed by Altura Credit Union in accordance with this Privacy Notices.

Relevant Privacy Notices and other resources

It is important that you read our other Privacy Notices on our website which may be relevant to you. In particular our Account Opening Privacy Notice, General Data Protection Privacy Notice, Lending

Privacy Notice and our 'Guidance on GDPR' and how we process your data beyond membership stage, if you are successful with your application.

GDPR- What does it mean?

Data protection has always been a priority for us and a core part of our business is keeping the data you entrust to us secure. This new regulation is designed to increase the level of transparency in how personal data is managed through and after, for example, the Member Onboarding process. We will always comply with the General Data Protection Regulation 'GDPR' when dealing with your personal data. Further details on GDPR can be found at Office of the Data Protection Commissioner's dedicated GDPR website (gdprandyou.ie).

Why is a Data Privacy Notice Required for Member Onboarding

To improve how we inform and communicate with our members in relation to data protection, we have prepared this Privacy Notice which sets out in more detail how your data is treated and managed at Member Onboarding stage and to provide you with information regarding the processing of your data for that purpose. A Data Privacy Notice is a document that every organisation who controls and processes personal information must make available. It details how we will collect, use, disclose, transfer and store your personal information during the Onboarding process.

Data Protection Impact Assessment- is there a risk to my data?

As a new technology is being introduced by Altura Credit Union for membership applications, Article 35(1) requires us to conduct a data 'impact assessment' to determine if there is any high risk to your data. A DPIA is a risk and compliance assessment of processing operations. As part of our compliance obligations, Altura Credit Union has reviewed, through a Data Risk Assessment, the online member onboarding functionality of the mobile app, to assess the lawful basis of processing your personal data and the level of appropriate technical and organisational measures that we have in place and as required under the GDPR. A detailed assessment of how your data is processed has therefore been carried out, including an analysis of the processing across the data protection principles. It provides a detailed record of the processing analysis carried out in order to identify the data protection risks. If you require any information on the risk analysis, please do not hesitate to contact the DPO at the details set out at the start of this Notice.

The assessment found that there were no residual 'high risks' to your data identified. The following was assessed in particular: Biometric data (i.e. facial recognition) and the fact that some of your data is transferred outside the EU. Of the risks identified by the assessment, we have established, through the assessment, how we can

- Improve transparency measures;
- Limit additional data collection;
- Implement an automated retention and deletion schedule so your data is removed automatically when it is no longer required;
- Implement additional security measures.

Can anyone use the APP?

The app is not designed to consider applications for Under 16s. The app will not process membership applications from someone other than you, so it cannot process third-party membership applications on your behalf. Therefore, you are the sole source of the data provided during the onboarding process.

Where do I fit in to the process of data collection and processing?

STAKEHOLDER	DATA PROTECTION ROLE	DESCRIPTION OF DATA
Altura Credit Union Ltd	Controller	All data collected as part of the member onboarding information collection and set out in this notice
Our Banking system software- 'Progress Banking Systems'	Processor	Provides the app functionality; through the banking software system
Jumio-- https://www.jumio.com/compliance-regulations/	Sub-Processor	They process identity documentation, i (name, address, DOB, age) and biometric measurements to verify identity documents
The App	Independent controller	Publication of the app
You- our valued member	You are the 'Data Subject', and whose information we protect	

What is the difference between the member onboarding option (through the APP), and attending at our Head Office at Mc Dermott Street, Gorey or at our branch offices?

The same information is collected as would be currently collected when someone applies in branch or in head office to join us. However, app related data is collected when someone downloads and uses the onboarding app. This data may include unique identifiers. Another difference is that documents can be provided electronically through the APP. You still however, have the option to join in person at head office or in branch. The lawful bases for processing your data through the Onboarding App are the same as the lawful bases for processing in-branch membership applications (with the exception that in-branch applications do not include special category biometric information).

Why do we collect and use your personal information for the Member Onboarding Process?

So that we can provide a more enhanced service. The service will also offer a number of efficient online services including an online banking service. You can use the app at your own convenience from home and you wont need to attend on site to join us. The service will facilitate Altura Credit Unions membership growth and facilitates our strategic objectives to benefit all our members.

We also gather and process your personal information for a variety of other reasons. For example, we use your personal information to process your membership application and (if your application for membership is successful) to: open an account (see our website for our 'Account Opening Privacy Notice' https://www.alturacu.ie/gdpr-and-you., to maintain an account for you, to help administer your accounts and services, and to ensure we provide you with the best service possible, to prevent unauthorised access to your account and to meet our legal and regulatory obligations. Some of these grounds for processing will overlap and there may be several grounds which justify our use of your personal data during the member onboarding process and for your relationship with us thereafter. Please do read our other privacy notices on our website which are all designed to inform

you. We will also require information to comply with our obligations under Credit Union Standard Rules. So, what are the legal bases for processing your data through the APP?

1. *To comply with a legal obligation*

Some of the processing of your data is required to comply with a regulatory requirement such as Anti-Money Laundering (AML) or tax regulations. When we process a membership application, we must comply with the Credit Union Act and with Anti-money laundering laws. Our legal obligations therefore apply to the Member onboarding process and indeed for your relationship with us afterwards. The following are some of the legal obligations we have:

a) **Regulatory authorities**: to report and respond to queries raised by regulatory authorities, law enforcement and other government agencies such as the Central Bank of Ireland;
b) **Credit Union rules:** To meet our obligations under Credit Union Standard Rules;
c) **Tax Regulation compliance**: to comply with tax regulations that require us to report the tax status of our members. We may share information and documentation with domestic and foreign tax authorities to establish your liability to tax in any jurisdiction. Where a member is tax resident in another jurisdiction Altura Credit Union has certain reporting obligations to Revenue under the Common Reporting Standard. Revenue will then exchange this information with the jurisdiction of tax residence of the member. We shall not be responsible to you or any third party for any loss incurred as a result of us taking such actions. Under the "Return of Payments (Banks, Building Societies, Credit Unions and Savings Banks) Regulations 2008", credit unions are obliged to report details to the Revenue in respect of dividend or interest payments to members, which include PPSN where held;
d) **Legal and Compliance**: to verify the personal information provided to us at member onboarding (and later at account opening stage) in order to meet our legal and compliance obligations, including to prevent money laundering, tax evasion, financing of terrorism and fraud. The information provided by you through the Member Onboarding App will be used for compliance with our customer due diligence and screening obligations under anti-money laundering and combating terrorist financing obligations under The Money Laundering provisions of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013 ("the Act") (and any subsequent AML legislation)
e) **Duties to our Regulator:** To meet our duties to the Regulator (the Central Bank of Ireland), we may allow authorised people to see our records (which may include information about you) for reporting, and compliance purposes. For the same reason, we will also hold the information about you when you are no longer a member. We may also share personal data with certain statutory bodies such as the Department of Finance, the Department of Social Protection and the Financial Services and Pensions Ombudsman Bureau of Ireland and the appropriate Supervisory Authority, if required under law.
f) **Audit:** To meet our legislative and regulatory duties to maintain audited financial accounts, we appoint an external and internal auditor. We will allow the internal and external auditor to see our account opening and membership records (which may include information about you) for these purposes.
g) **Investigation or legal proceedings**: to co-operate with and provide information requested to legal and/or regulatory authorities in the context of investigations or proceedings;
h) **Record retention**: to keep records of communications, account opening forms and member account activities;
i) **Registration :** to maintain a register of members of Altura Credit Union;

j) **Operations:** to administer our internal operational requirements (including membership, credit, compliance and risk management, system development, staff training, accounting and for audit purposes);

k) **Member communications:** to communicate certain information to you such as providing notice of the AGM or sending you an annual account statement;

l) **Security**: to undertake systems testing, maintenance and development in order to ensure network and information security;

m) **Nominations:** The Credit Union Act 1997 (as amended) allows members to nominate a person(s) to receive a certain amount from their account on their death, subject to a statutory maximum. Where a member wishes to make a nomination, Altura Credit Union must record personal data of nominees in this event.

n) **Incapacity to Act on your account following a successful onboarding membership application**: The Credit Union Act 1997 (as amended) provides, in the circumstances where you become unable to transact on your account, due to a mental incapability and no person has been legally appointed to administer your account, that the Board may allow payment to another who it deems proper to receive it, where it is just and expedient to do so, in order that the money be applied in your best interests. In order to facilitate this, medical evidence of your incapacity will be required which will include data about your mental health. This information will be treated in the strictest confidentiality.

2. <u>To enter into and perform a contract with you for the services which you require</u>

Processing through the APP is also carried out for the purpose of entering into a contract with Altura Credit Union and you will need to adhere to Altura Credit Unions rules (which are the same rules used for in-branch applications). As we operate in a regulated sector, there are many contractual considerations. This basis is appropriate where the processing is necessary for us to manage your membership and accounts and credit union services. In order to consider your application for membership of Altura Credit Union (and your relationship with us thereafter) and to process any product/service applications you may make, we have to gather and process some personal information during the onboarding process and some data is processed after the process and for the purpose of maintaining an account. Please see our other privacy notices and the contexts in which the processing of your data arises. The following are some examples:

(a) Administrative Purposes: We will use the information provided by you through the APP, for the purpose of assessing your Onboarding application.

(b) Third parties: An external third party (Progress Banking Systems) is required to undertake Member Onboarding operational functions on our behalf (for example our banking system). We will ensure that any information passed to such third parties will be done for the security of your data and will be protected in line with data protection law.

(c) Irish League of Credit Unions (ILCU) **Affiliation:** The ILCU (a trade and representative body for credit unions in Ireland and Northern Ireland) provides professional and business support services such as marketing and public affairs representation, monitoring, financial, compliance, risk, learning and development, and insurance services to affiliated credit unions. As this credit union is affiliated to the ILCU, Altura Credit Union must also operate in line with the ILCU Standard Rules (which members of Altura Credit Union are bound to Altura Credit Union by) and the League Rules (which Altura Credit Union is bound to the ILCU by). We may disclose information in respect of any account or transaction of yours from the date of your original membership to authorised officers or employees of the ILCU for the purpose of the ILCU providing these services to us

(d) The ILCU Savings Protection Scheme (SPS): We may disclose information from the date of your original onboarding membership application, to authorised officers or employees of the ILCU for the purpose of the ILCU providing these services and fulfilling requirements under

our affiliation to the ILCU, and the SPS. The Privacy Notice of ILCU can be found at www.creditunion.ie

(e) Electronic Payments If you use our electronic payment services to transfer money into or out of your credit union account which you open during your membership process (such as a 'share account'} or make payments though your debit card into your, we are required to share your data with our electronic payment service provider;

(f) Member Service: We may use information that you provide to help us improve our services to you

(g) Insurance: As part of our affiliation with the ILCU, we purchase insurance from ECCU Assurance DAC (ECCU), a life insurance company, wholly owned by the ILCU. To administer these insurances, we may pass your information to ECCU and it may be necessary to process 'special category' personal data about you. This includes information about your health which will be shared with ECCU for the purposes of our life assurance policy to allow ECCU to deal with insurance underwriting, administration and claims on our behalf. Further information can be found in our lending privacy notice.

(h) Debit Cards etc: If you will have a Debit Card or prepaid card with us, we will share transaction details with companies which help us provide this service.

3. To enable Altura Credit Union to function as a business

A legitimate interest is when we have a business or commercial reason to use your information. Specifically for the purposes of the Membership onboarding application however, the processing of your data is not carried out on the basis of any 'legitimate Interests'. For other data processing situations based on legitimate interests (such as Telephone records, services Information, CCTV and Voice Recording for example), please see our General Data Protection Privacy Notices on our website.

4. *Consent*

The processing of additional information via the app, especially the biometric information, is optional and you can alternatively complete the application by verifying your ID documentation using the normal paper process at Head Office or in branch. Explicit consent is a valid lawful basis for processing your data under Art 9 of the GDPR. Through the APP we therefore seek your consent for the use of the Biometric data. We also seek your consent for electronic AGM notifications, annual account statements, and online access. We will only carry out processing when we have obtained your express consent and will cease processing once you withdraw such consent. You can at any time withdraw consent by contacting us. Full contact details are provided at the start of this notice, or you can contact the MSO at 0539488700. For other data processing contexts that reply on your express consent, see our General Data Protection Privacy Notice on our website. Other consent options arising for you through the onboarding APP also includes:

(a) Text marketing consent:
(b) Email Marketing consent;
(c) Phone marketing consent;
(d) Post marketing consent;
(e) Members monthly Draw.

What Personal Information we collect about you

The collection of the data is triggered when you download the mobile app. The data is either collected from the you directly or generated as a result of your actions (date and timestamps / application status information). As mentioned above, you have an option to partially complete your membership application via the app, and to provide proof of ID, proof of address and proof of PPSN

documentation in person at our Head Office or in branch. The information to be collected via the app is as follows:

Membership:
Membership information is collected for all applications.
Title; First Name; Middle Name; Surname; Address; Country of Residence; Accommodation; Date of Residency Previous Address; Country of Residence; Email Address; Mobile Number; Home Phone Number; Date of Birth; Country of Birth; Nationality; Gender; Marital Status; PPS Number;

Family member information is also collected
Family member information is collected where a member qualifies because of their relationship with an existing member. Data collected is: Family Member Number; Family Member First Name; Family Member Surname; Family Member Relationship; Family Member Address; Family Member Phone Number.

Employment Status
Employment Status information is collected when you qualify because you work in our common bond area. Employer information is required to confirm this as follows: Occupation ID; Employer Name; Employer Address.

Beneficial ownership; PEP (Politically Exposed Person) and Source of Funds information
Data collected is : Member Beneficial Owner Title; Beneficial Owner First Name ;Beneficial Owner Middle Name; Beneficial Owner Surname; Beneficial Owner Address; Beneficial Owner Country; Beneficial Owner Date of Birth; Beneficial Owner Relationship; Beneficial Owner Contact Number; Beneficial Owner PPS; Beneficial Owner Country of Tax Residence; Beneficial Owner TIN; Beneficial Owner Member a PEP? PEP Details; Reason for Joining; Member Payment Type; Source of Funds Type; Source of Wealth Type; details concerning Tax Resident; Country of Tax Residence TIN.

Member preferences and Confirmations
Consent to Keep Applicant Photo; Confirm Depositor Guarantee Scheme Regulations; Reason for Joining; Text Marketing Permitted; Email Marketing Permitted; Phone Marketing Permitted; Post Marketing Permitted; Opt-Out Promotion (Sign up for monthly draw); Sign UP for Online Access Preference; Electronic Statement Prefer; Electronic AGM Booklet.

Nomination Information (when introduced- not presently a facility)
Nomination First Name; Nomination Middle Name; Nomination Surname; Nomination Address; Nomination Date of Birth; Nomination Relationship; Nomination Details; Nomination Contact Number; Is Nominee Member.

Identity documents and document verification
Proof of address document / photo / scan; Proof of PPSN (Optional)document / photo /scan Identity document; Photo taken on device with biometric measurements.

Data Minimisation- How can I be assured that Altura Credit Union is not excessively collecting data?

How will the data be used?
The data is used by us to process new member applications. We need to be satisfied that you meet the requirements of our common bond and that you are eligible for membership, that you have provided all the information required to become a member and that you have met all statutory requirements including providing proof of identity. Altura Credit Union collects employment details

(status, occupation and employer name), even if you are living in the common bond. Our AMl and Regulatory requirements are the reason we collect this additional information.

How we use particularly sensitive personal data

The processing of Special Category Data (Bio-Metric Data) is only performed with your consent through the APP. The risk assessment conducted for Member APP Onboarding closely examined the use of sub-processors known as 'Jumio' which is a California-based company with global operations including operations in the US and India. Jumio processes the Bio Metric data. Their processing involves the collection of your biometric information in order to validate your identity. For information on Jumio please see their website: https://www.jumio.com/compliance-regulations/

Profiling

The Automated-decision making process makes decisions on your application and there is therefore the use of profiling or algorithmic means to determine your access to our services. Member onboarding therefore does use systems to assist a decision based on personal data we have about you through the onboarding process.

How we use personal information for direct marketing

From time to time, we would like to make you aware of other services that we offer, which may be of interest to you during the onboarding process. For this reason, you will be given optional marketing preferences.

Who we share your information with

We may share your personal information with trusted third parties who perform important functions for the performance of the APP and appropriate confidentiality and security measures are applied through Data Processing Agreements in compliance with GDPR.

Progress Banking Systems

Progress Banking is installed in **many credit unions in Ireland and the UK. They** provide all the functionality and services required to process your onboarding membership application with Altura Credit Union.

Jumio

Progress have a contract with Jumio. The risk assessment closely examined their use of Jumio which is a Californian based company having its operations in the US. You can learn more about Jumio by going to their website at https://www.jumio.com/compliance-regulations/. They process the Biometric data necessary to establish your identity. Some web and mobile data will also be shared but this is limited to data about the download and usage of the app, and does not include any of your data collected for the purposes of the membership application.

Who else do we share your data with

We limit the disclosure of your information to regulatory disclosures e.g Central Bank, CCR, MLRO Reporting and Revenue. For details of other processors who we may share your data with (following a successful Member Onboarding application), see our General Data Privacy Notice on our website.

How secure is my information with third-party service providers?

Data is shared between the app, Progress Banking system and the sub-processor (Jumio) using encrypted links. Jumio and Progress (our banking software providers) encrypt all your data in transit

and Jumio encrypts all of your data 'at rest'. All our third-party service providers are required to take these appropriate security measures to protect your personal data in line with our policies.

Progress banking systems

Progress Systems have been assessed and certified as meeting the requirements of **ISO27001** for the provision of computer software, hardware and support to Altura Credit Unions and they are subject to satisfactory surveillance audits. Vulnerability and a Penetration Test of their Internet Banking Service is regularly conducted to ensure there is no risk to data**.** Progress' Information Security Management System (ISMS) was certified to ISO/IEC 27001:2005 in 2012. In 2015 they upgraded their ISMS to the ISO/IEC 27001:2013 standard. Each year their ISMS has been subject to a surveillance audit to ensure adherence to the ISO 27001 standard ensuring the highest awareness of data protection for Altura Credit Union Ltd. There is also an existing data processing agreement between Altura Credit Union and Progress Software which incorporates the member onboarding processing activity. Access controls are enforced by our banking software and the data collected is processed within our banking software. We do not allow our third-party service providers to use your personal data for their own purposes, unless they are deemed to be controllers in their own right. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Jumio

Our providers are also bound by confidentiality obligations. Identity verification is very important in the new member onboarding process, and this app provides two mechanisms to ensure that this verification can be achieved through the online process (a) validation of your mobile phone associated with the account and (b), verification of your identity document through Jumio. This is done via a one-time-password generated and sent to you via SMS. You must type this password and send it back to the server for validation. The password has an expiry period. A desk-based assessment was carried out on Jumio. App penetration tests have been carried out and will be ongoing to ensure the integrity of your data. Only Irish Mobile numbers are used which restricts opportunities for fraudulent use of your data. All data is encrypted at all times in transit and on the banking system.

Other jurisdictions- is my data transferred outside Ireland?

The people and organisations that we may share your personal information with may be located in a country that does not have data protection laws which provide the same level of protection as the laws in Ireland. Some countries already have adequate protection for personal information under their applicable laws. In other countries safeguards will be applied to maintain the same level of protection as the country in which the products and services are supplied. These safeguards may be contractual agreements with the overseas recipient or it may require the recipient to subscribe to international data protection frameworks. For more information about the European Commission's decision on the adequacy of the protection of personal information in countries outside the EEA, please visit: https://ec.europa. eu/info/law/law-topic/data-protection_en

Through this APP, Data is transferred across borders outside the European Union. The sub-processor (Jumio) is US based, so there is potential for your data being transferred to the US and India. Transfer mechanisms as well as information about the processing locations were therefore examined as part of the risk assessment and no high residual risks were found.

Is providing your personal information obligatory?

We are unable to enter into or administer the onboarding relationship with you without some personal information about you. In cases where providing your personal information is optional we will make this clear through the process. In particular, it is not mandatory that our members sign up

to receive marketing communications. If you fail however to provide certain other onboarding information when requested, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations.

Updates to your personal information

If any of the personal information you have given to us at onboarding or account opening stage should change thereafter, such as your contact details, please inform us without delay. Similarly, if we have collected personal information about you at onboarding or account opening stage that you consider to be inaccurate, please inform us. Our contact details are set out at the beginning of this document.

How long we keep your personal data for

If you initiate an online member application, but you stop before providing the supporting documentation, the partially completed application will expire within a time period of 7 days. A reminder notification and/or email will be sent to you, but the data will be erased from the banking system once the application expires. Jumio will retain data for 5 days because it allows the Jumio process to complete. The data is stored locally on your device until you reach a certain point in the application process when the data collected to that point is transferred directly to our Progress banking system. Information collected after that point e.g your membership supporting documentation, is uploaded to our system once it is verified through the Jumio application. This data will be deleted by Jumio 5 days thereafter. Your data is not transferred into our Banking system until you have completed all the data entry screens and when you have actively initiated the membership application. Up to this point it is stored locally on your phone. When the data is uploaded to our banking system it will appear in a queue. Our banking system will flag your application if you do not progress it, and will autodelete it after 7 days

We need to keep/store your personal information for as long as necessary to fulfil the onboarding purposes for which it was collected (as described above) taking into account any legal/contractual obligation to keep it. The criteria we use to determine data retention periods for your personal information through the process includes retention in case of queries i.e. we will retain for 7 days in case of queries from you (for instance, if you submit an application and if that is unsuccessful).

Examples of Retention Periods

For the duration of your relationship with us (and thereafter) please see our other data retention periods as follows

Membership Application	7 Years after relationship has ended
Member onboarding	7 days for rejected or withdrawn applications
Nomination Forms	7 Years after relationship has ended
CCTV recording which is used in the normal course of business (i.e. for security purposes).	One Month
Copies of ID Proof of Address	5 Years after relationship has ended
Loan application forms	7 Years from date of discharge, final repayment, or transfer of loan
Loan Supporting Documentation	7 Years from breach, satisfaction or expiration
Credit Agreements	7 Years from breach, satisfaction or expiration – 12 years if under seal

ICB checks	5 Years from date of receipt
Telephone recordings	30 days
CCR Enquiry	5 Years from date of access
Rescheduled Loan Request	7 Years
Guarantees	7 Years from the date of default
Lodgement/Withdrawal documents	5 Years
Member Complaints	6 Years after the complaint has been resolved
Loan Protection/Life Savings Claims Documentation	6 Years after the relationship has ended
Income tax records	We keep **income tax** records for a period of six years after completion of the transactions to which they relate.
Accounting records	required to be kept further to Altura Credit Union Act, 1997 (as amended) must be retained for not less than six years from the date to which it relates.
Declaration of Health Forms	Until loan is repaid or a new DOH completed and approved

Your rights under data protection laws

You can be assured that we will only use your data for the purpose it was provided through the onboarding process and in ways compatible with that stated purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please see our website for a guide to your rights. You have several rights in relation to how we use your information as follows:

To find out whether we hold any of your personal data and **if we do to request access** to that data that to be furnished a copy of that data. You are also entitled to request further information about the processing.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you rectified.

Request erasure of your personal information. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.

Request the restriction of processing of your personal information. You can ask us to suspend processing personal data about you, in certain circumstances.

Where we are processing your data based solely on your consent **you have a right to withdraw that consent at any time and free of charge**.

Request that we: a) **provide you with a copy of any relevant personal data in a reusable format**; or b) **request that we transfer your relevant personal data to another controller** where it's technically feasible to do so. **'**Relevant personal data is personal data that: *You have provided to us or which is generated by your use of our service. Which is processed by automated means and where the basis that we process it is on your consent or on a contract that you have entered into with us.*

Please note that the above rights are not always absolute, and there may be some limitations

If you want access and/ or copies of any of your personal data or if you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we send you or a third party a copy your relevant personal data in a reusable format please contact our Data Protection Officer (contact details at the beginning of this Notice). Alternatively call in to us and our officers will help you.

Do I pay a Fee?

There is no fee in using any of your above rights, unless your request for access is clearly unfounded or excessive. We also reserve the right to refuse to comply with the request in such circumstances.

Identification

We may need to verify your identity if we have reasonable doubts as to who you are. This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

Updates

This Data Privacy Notice may be updated from time to time and the current version of this Data Privacy Notice shall be displayed on our website. **Updating this Privacy Notice** Amendments will not be made retrospectively.

Contact for Inquiries

We want the Member Onboarding service to meet your expectations at all times. Please help us by telling us straightaway if there are any changes to your personal information. If you wish to avail of any of your rights set out by this Notice, please contact: Donal O'Connor, Data Protection Officer at Altura Credit Union Limited, Mc Dermott Street, Gorey County Wexford email dp@alturacu.ie or telephone 0539488700

Complaints		
You have a **right to complain** to the **Data Protection Commissioner** in respect of any processing of your data. The Data Protection Commissioner has enforcement powers and can investigate compliance with data protection laws		
Post Data Protection Commissioner Canal House Station Road Portarlington R32 AP23 Co. Laois	**Telephone** +353 (0)57 868 4800 +353 (0)761 104 800 1890 252 231	**E-mail** info@dataprotection.ie

End of Privacy Notice