Microsoft

General Data Protection Regulation (GDPR) Considerations for Customer Facing Applications

February 2019

Contents

Introduction

The General Data Protection Requirement (GDPR) is a European Union regulation adopted April 14, 2016 to protect individuals and their personal data. The grace period for implementation ended on May 25, 2018.

For any customer facing applications, GDPR must be taken into consideration by all organizations that embark on projects that hold personal data and serve EU citizens. Every organization must allow individuals to consent to the storing of personal data in compliance with GDPR. Personal individual data relates to anything that identifies a person, and which needs specific compliance for the processing and control of the data and how it is shared. GDPR applies to all EU and European Economic Area (EEA) member states and must be implemented by every company that holds and processes personal individual data. Any company that offers goods and services to EU and EEA member states individuals must comply with GDPR, even if they do not reside within the EU or EEA member states. Any company failing to comply with the GDPR regulation can incur a monetary penalty to the company processing or holding the personal data.

Microsoft's Azure Active Directory B2C (Azure AD B2C) is a cloud identity and access management solution for your web and mobile applications. It is a highly available global service that scales to hundreds of millions of identities. Built on an enterprise-grade secure platform, Azure AD B2C keeps your applications, your business, and your customers protected. This solution guide focuses on how Microsoft Azure Active Directory B2C can be leveraged as one component of GDPR considerations for customer facing applications.

> **Note:** This paper builds on a basic understanding of Azure AD B2C and its capabilities. You can read more about this consumer identity platform here: https://azure.microsoft.com/services/active-directory-b2c/
>
> To learn more about developing solutions with Azure AD B2C, see Gaining Expertise with Azure AD B2C, a self-paced course for developers.

Solution Overview

Azure AD B2C can be used as a flexible component of your overall strategy. Before we dive deeper, let us first introduce some of the nomenclature used to describe the tools and capabilities of the platform that you will use to implement GDPR-compliant flows.

Common Azure AD B2C Capabilities and Nomenclature

User Journey

A user journey is your customer's experience and interaction with the identity and authentication experiences that you build using Azure AD B2C. Examples of journeys include signing up for your service, signing in to access your app, or updating their profile with more information about themselves.

User Flows and Custom Policies

The Identity Experience Framework (IEF) of Azure AD B2C is a core strength of the service. User flows and custom policies are the programmatic description of a user journey. For instance, a sign-up user flow allows you to control behaviors by configuring the following settings:

- Account types (social accounts such as Facebook, Google, LinkedIn, or local accounts such as the user's email addresses or a username and a password) that consumers can use to sign up for the application
- Attributes (for example, first name, postal code) to be collected from the consumer during sign-up
- Use of Azure Multi-Factor Authentication
- The look and feel of the sign-up pages
- Information that the application receives when the user flow run finishes

You can create multiple user flows of different types in your Azure AD B2C environment (also called a tenant) and use them in your applications as needed. User flows can be reused across applications. This flexibility enables developers to define and modify consumer identity experiences with minimal or no changes to their code.

You can create these user flows either through a user interface in the Azure Portal (built-in user flows) or alternatively, you can craft more complex journeys using a declarative XML schema (custom policies). This schema is defined in the Identity Experience Framework that comprises custom policy parsing rules, as well as the rest of the scaffolding required to enable Azure AD's consumer identity functionality. Click here for more information on the two ways to author user journeys:

- [Built-in User Flows](#)
- [Custom Policies](#)

Microsoft Graph API

The Microsoft Graph API provides programmatic access to Azure AD B2C (in addition to the rest of the [Microsoft 365 Suite](#)) through REST API endpoints. Applications can use Microsoft Graph API to perform create, read, update, and delete (CRUD) operations on directory data

and objects. To begin using the Azure AD Graph API, take a look at the [Azure AD B2C Graph API Documentation.](#)

The Key GDPR Rights for an Individual

The GDPR sets forth a set of key rights for an individual, known as a subject in the GDPR legislation, for storage and processing of their personal information. These include:

- **Individuals must explicitly opt-in to their information being shared with 3rd parties**. Individuals must initially consent to and be able to withdraw consent for sharing data with 3rd parties.
- **Right to Access.** Individuals have the right to see and edit all data associated with their identity. Data portability ensures they receive data in an industry standard format, and they have the right to transmit this data to another service.
- **Right to be Forgotten.** Individuals have the right to request the deletion of all data related to their identity.
- **Breach notifications must be communicated.** The company must inform users of any breach of the service within 72 hours of the discovery of the breach.
- **A data protection officer (a type of internal auditor) must be appointed.** Every organization that engages in large scale processing of sensitive personal data must appoint a Data Compliance Officer (DPO). A DPO must have the appropriate tools to monitor compliance. They must be able to cooperate with requests from the supervisory authority.
- **Minors must have parental consent.** individuals who are minors must have parental consent to use a service, regardless of its intended audience.

This is not a comprehensive list, read more about GDPR here (http://www.eugdpr.org/).

Over the next several sections, we will dive into each of these key rights and discuss the functionality Azure AD B2C provides that support each right, and the additional work your organization will need to do to ensure your customer facing applications achieve GDPR compliance.

> **Important!**
> **The features in Azure AD B2C can be used in specific ways to support the data subject rights. In the context of GDPR, Azure AD B2C is a data processor. This document describes implementation details that may be of assistance to data controllers while building applications using Azure AD B2C. Consult with your legal counsel for legal advice on GDPR. In this document "You" refers to the data controller (aka service provider and application owner).**

Consent to share data with 3rd party services

This right state that consent must be given explicitly for sharing end user information with 3rd parties. Users must opt-in to this sharing. The end user must also be able to withdraw consent for sharing their data at any time. The user must consent if data is to be shared with additional third parties not included in the original consent.
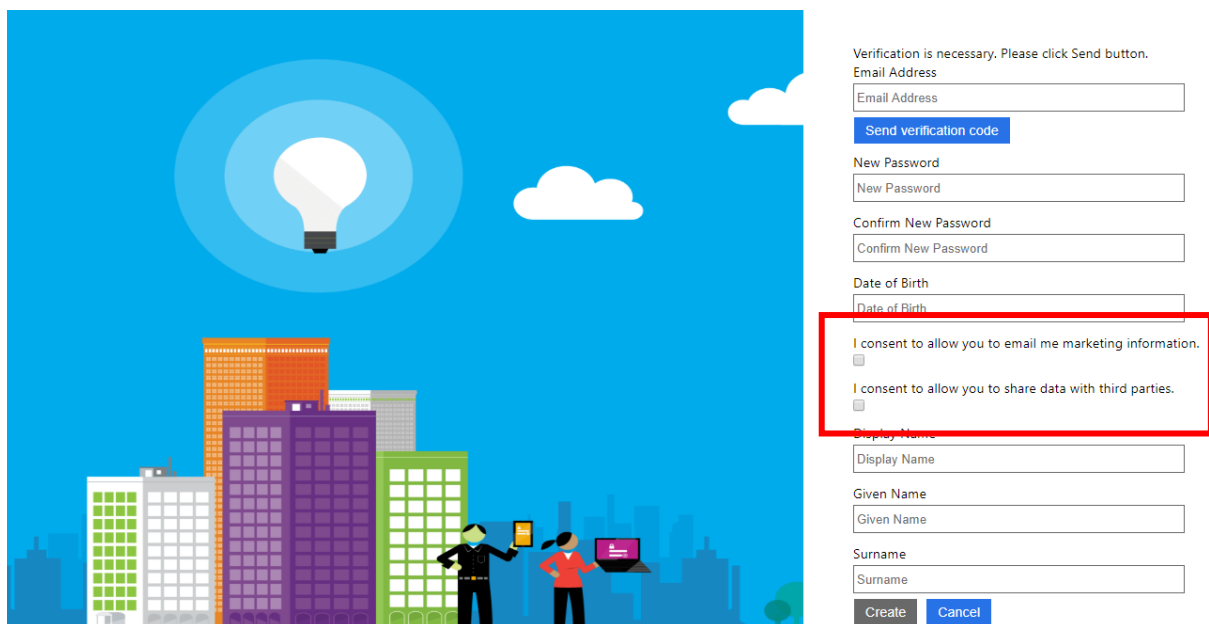
Enabling Functionality Available in Azure AD B2C

You can configure Azure AD B2C to obtain consent from your users to share data with 3rd parties using user flows. Here are some specific consent-related actions you can specify in an Azure AD B2C User Flow:

- Consent can be collected as part of all registrations (i.e. signup) and persisted in the directory.
- Consent can be collected if it is missing or has expired during an authentication journey (i.e. sign-in).
- Consent can be withdrawn using a profile-edit user flow where a user can change their consent options.
- Access to the app can be blocked by Azure AD B2C if consent is declined.
- A record of user consent to share data with 3rd parties may be stored in the Azure AD B2C directory as an extension attribute.

  Note: Several of these abilities only apply to new sign-ups in Azure AD B2C when using built-in user flows. Collecting consent from existing customers or updating consent for additional third parties requires that you use custom policies.

Following is an illustration of what the consent experience might look like once it is configured:

Work required in your organization

- Your organization should take inventory of all situations in which data is shared with a 3rd party.
- You may choose to collect permission to share data with specific 3rd parties during sign-up for the service. For example, a user may need to select a checkbox to agree to the Terms of Service that lists 3rd party services that will have access to the user's personal data. It is also possible that your application will collect permission to share

data with 3rd parties when appropriate (a specific feature may require a 3rd party service).

For detailed [developer guidance](#) on how to implement this flow, please refer to the Developer Guidance section below.

GDPR Right to Access / Data Portability (GDPR export)

Right to Access empowers end users to request and receive a copy of their personal data. Data Portability ensures that they receive data in an industry standard format, and that they have the right to transmit this data to another service.

Additionally, the GDPR gives rights to people (known in the regulation as data subjects) to manage the personal data that has been collected by an employer or other type of agency or organization (known as the data controller or just controller). Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of it, requesting changes to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a Data Subject Request or DSR.

Enabling Functionality Available in Azure AD B2C

- You can use the Microsoft Graph API to export users' directory data from Azure AD B2C in real time.
- You can also download application usage logs (aka Audit logs) using the [reporting API,](#) filtered by the object ID of a user and make it available to the end user for them to review.
- An end user may log in to an Azure AD B2C registered application, select a "Profile Edit" user flow and review and edit most of their own directory provided data as part of an Azure AD B2C profile edit user journey.

Work required in your organization

- Your business is responsible for accepting a GDPR export request. You may choose to do this programmatically through a web experience, or as part of an over-the-phone support call.
- You must invoke the Microsoft Graph API with the correct User Object ID to obtain the directory data and invoke the Microsoft Graph Reporting API (Audit data) to obtain the audit logs for a user
- Your organization is responsible for exporting any data associated with that user that exists outside of Azure AD B2C. This includes all data associated with that individual that exists in applications, CRM systems, backups, and telemetry.
- Your organization must supply a means to deliver this data to the individual. You may decide to make this data securely available through your website, or your support team may have a means to share large files with consumers.

- Issuing a Data Subject Rights (DSR) requires a unique user identifier such as user object ID. This representation of the user must be persisted in your user directory to perform DSR actions such as export or delete.

For detailed developer guidance on how to use Graph to export user data, please refer to the [Developer Guidance](#) section below.

GDPR Right to be Forgotten (GDPR delete)

Right to be Forgotten allows an end user to request the deletion of all their personal data stored by a data controller. *You must make the Graph API call on the same day you receive it to ensure compliance with the requirement for deletion within one month.*

Enabling Functionality Available in Azure AD B2C

- The DELETE command in the Microsoft Graph API enables a service provider to delete all the directory data for a user in response to a qualified request. The default delete request is a soft-deletion. The user is no longer able to log in, and the user data will no longer be returned by standard Graph API calls. The user data will be permanently deleted 30 days after the soft-delete is performed. During this time, the user can be restored or permanently deleted using the Azure Portal. When permanently deleting a user, in most cases, the data will be deleted within one day.
- Non-directory data consists of usage logs. Usage log (AKA Audit log) events older than 30 days are deleted automatically by the Azure AD B2C service for all users. Most companies download this data to internal analysis tools to track telemetry and other information important to their business.

Work required in your organization

- Your business is responsible for implementing a mechanism to accept a GDPR delete request. You may choose to do this programmatically through a web experience, or perhaps as part of an over-the-phone support call.
- You must invoke the Azure AD B2C GDPR Delete API with the correct User Object ID and an application registration that has been granted specific delete permissions over user objects.
- Your organization is responsible for deleting any data associated with that user that exists outside of Azure AD B2C. This includes all data associated with that individual that exists in applications, CRM systems, backups, etc.

For detailed developer guidance on how to use Graph to delete user data, please refer to the [Developer Guidance](#) section below.

GDPR Breach Notification

Breach notification must be communicated within 72 hours of having become aware of a breach.

Enabling Functionality Available in Azure AD B2C

In the event of a breach, Microsoft will contact the Azure subscription owner as well as the security contact specified. This requires that the Azure AD B2C tenant be linked to an Azure subscription and that the information is up to date.

Work required in your organization

- To be contacted as soon as possible after a data breach complete the following:
    1) Ensure that your Azure AD B2C tenant is [linked to your Azure subscription](#).
    2) In your regular Azure AD tenant, from the Azure Portal, open **Security Center**, then open **Recommendations** and select **Provide security contact details**. Select the subscription linked to your Azure AD B2C tenant. Enter your organization's security contact information. See: [Detailed instructions on providing security contact information to Azure](#).
- Establish a process for your organization to communicate a data breach to your affected consumers within 72 hours. You can expect that Microsoft will be able to provide a list of impacted accounts in the form of a .CSV file.
- Microsoft will need your data protection officer(s) contact information on file to engage with your company within 24 hours. It is expected that your data protection officer(s) will be available even during non-business hours.

GDPR Parental Consent

Applications need a consent mechanism to allow access for minors. Minors must have consent from a parent to use any service, regardless of whether it's targeted at minors. Telemetry, analytics and targeted marketing must be disabled for minors even after parental consent.

Azure AD B2C [supports age gating in basic user flows](#) or age gating can be implemented with custom policies. While Azure AD B2C can collect an individual's date of birth to determine age, it does not support verification of age to provide parental consent. Your app will need to handle this, or you will need to utilize a third-party solution. Azure AD B2C supports the notion of an account having parental consent but does not directly provide the ability to link accounts. Once an age classification is determined, Azure AD B2C provides support for several possible behaviours for your app, including blocking the authentication or providing a limited response without storing data.

Enabling Functionality Available in Azure AD B2C

Parental consent and age-gating are implemented in Azure AD B2C using a combination of tenant configuration in the Azure portal and through Microsoft Graph. Following are the specific functions you can perform using Azure AD B2C:

- Collecting Date of Birth and Country for all users to determine if the user is a minor. This information can be collected during sign-up for new users, or during sign-in for existing users if Date of Birth and Country have not been previously collected.
- Blocking minors from signing up from your service if that is the desired behavior.

- Issuing id tokens with a claim indicating that the user is considered a minor. This will take into consideration that different countries have different laws about what age is considered a minor.
- Invoking a third-party parental consent service.
- Storing a child's parent data in the directory through the Graph API.
- Enabling and disabling of a child's account through the Graph API. This will be possible by flagging an account as **minor without parental consent.**
- GDPR delete of a child's account as described earlier under GDPR Right to be Forgotten.

Work required in your organization

- Your organization may choose to block minors from using your application. If your application needs to collect a minor's personal data with respect to a transaction or activity within an EU territory, then the rest of the implementation guidance in this section may apply.
- Through your application or another service, your organization must provide a parental consent system capable of collecting consent from the parent on behalf of the child. For Azure AD B2C to enforce this consent requirement, the status of the consent must be recorded to the Azure AD B2C directory in an extension attribute.
- Some organizations will choose to collect and process Data Subject Rights using a manual process such as calling a support hotline. Your organization may instead choose to implement a collection of these requests in your app.
- Your organization must accept a parent's request to export all data in a child's account. This request must be serviced by calling a Graph API in Azure AD B2C as well as exporting any of the child's personal data maintained by the application or organization.
- Your organization must accept a parent's request to delete a child's account and all personal data. This request must be serviced by calling a Graph API in Azure AD B2C as well as deleting any of the child's personal data maintained by the application or organization.
- In the event of a data breach of a child's account, the parent of the child must be notified within 72 hours.
- Your application may need to behave differently for minors. Your organization may need to disable direct marketing or profiling using data from minors even after parental consent. Azure AD B2C can be configured to issue tokens that identify minors so that your application can act accordingly.

For detailed developer guidance on how to use Graph to implement parental consent based on age gating, please refer to the Developer Guidance section below.

Other GDPR Considerations

In addition to complying with the five key rights, your organization will also need to create systems to achieve the following:

- A service for tracking all systems within your organization that have data for any given individual.

- A mechanism for accepting and coordinating GDPR Data Subject Right (DSR) requests across all systems in your organization.

Solution Planning

User Journey to GDPR Requirement Mapping

The following table illustrates how User Journeys and user flows are connected to GDPR requirements and summarizes the Azure AD B2C and Microsoft Graph support of the requirements.

GDPR Requirement	Associated User Journeys and User Flows	Azure AD B2C and Microsoft Graph Support
Opt-in to sharing of data	Sign-up/Sign-in Sign-in Profile Edit	• Collecting consent as a part of sign up and/in sign up to the application. • Presentation of Terms and Conditions, including consent. • Storing of consent, and consented versions. (requires custom policies) • Blocking access to the application if consent is not granted.
Right to access/Data Portability	Profile Edit	• Users may view and edit their directory information.
	Outside of user flows	• Microsoft Graph API can be called to export all user directory data for a specific User Object ID. • Audit log can be downloaded and filtered to a user ID.
Right to be forgotten	Outside of user flows	• Microsoft Graph API Delete command deletes all directory data for the user. • Non-directory usage/audit logs automatic deletion every thirty days.
Parental consent for minors	Sign-up/Sign-in Sign-in	• Collection of Date of Birth and Country for all users to determine minor status. • Blocking of minors from signing in.
	Outside of user flows	• Issuing ID Tokens with a claim indicating user is a minor, based on country. • Verifying parental consent and storing in the consentProvidedForMinor field using a Graph API call • Storing a child's parent data in the directory through the Graph API

		• Enabling and disabling a child's account by flagging as **minor without parental consent**
Breach Notifications	Outside of user flows	• Microsoft will contact your designated security contact within one day.

Developer Guidance - User Flows

These samples will provide details on how to support the GDPR requirements in Azure AD B2C. These will go over the sign-up and profile edit user flows, which apply to the GDPR requirements regarding consent to share data, the ability to revoke that consent, and understanding that a user is a minor.

These samples will provide a mechanism to store user consent for email marketing and sharing data with third parties, as well as the user's date of birth to determine their age, and their country of residence.

There are two steps you need to take to support the GDPR components into the user journeys for sign-up and profile edit.

- Create the attributes in Azure AD B2C
- Use the attributes in the User Journeys

Depending on the work flow within your app, you may or may not want to provide the GDPR attributes to your app. Another app, such as a marketing app, may need to use the Graph API to find users who have consented to email marketing or sharing data with third parties.

Differences between User Flows and Custom Policies

Built-In user flows in Azure AD B2C support many basic authentication flows. Custom policies provide the capability to perform some logic based on the identity data held by Azure AD B2C. This allows for a richer experience than the built-in user flows can provide. There are multiple scenarios that require the additional capabilities of custom policies.

The following requirements can only be satisfied by using custom policies:

- Integration with external APIs
- Integration with SAML Identity Providers
- Prompting for consent for existing users, including versioned consent
- Migrating users

Age Gating

Age gating is a feature supported by built-in user flows which allows Azure AD B2C to identify minors in your app. You can choose to block the user from signing in or signing up or pass additional claims back to your app indicating the users age group and parental consent status.

Attribute Creation

You can create attributes in Azure AD B2C in one of two ways: You can use the Azure Portal UI to create attributes, or you can create attributes programmatically using the Graph API. To use the Graph API, please refer to the documentation.

Using the Azure Portal UI is easiest to add attributes if only a few attributes are being created and will be presented here.

In your Azure AD B2C tenant, using the Azure AD B2C blade, select the "User attributes" section.

Here, you will add the required attributes. This will allow Azure AD B2C to store the data for the attribute with the extensions application that is used for custom attributes.

 You can refer to the documentation as you define the following attributes:

Name	Type	Description
DateOfBirth	String	Date of Birth – used to determine age
emailMarketing	Boolean	Used to store consent to email the user
shareDataWithTP	Boolean	Used to store consent to share data with third parties

The samples use the country attribute, however this attribute already exists in the standard Azure AD B2C attributes.

Update User Journeys

Built-In User Flows

Sign-In / Sign-Up User Flow (with samples)

You will want to create a sign-up or sign-in user flow with the following settings.

User Flow Section	Settings
Name	GDPR_Sample_SUSI
Identity Providers	• Email signup
Sign-Up attributes	• Any attributes you want to collect • DateOfBirth • Country/Region • emailMarketing • shareDataWithTP
Application claims	• Any claims you want to pass to your app, including any GDPR claims
Page UI customization	Update the Local account sign-up page attributes to use an appropriate input field, either drop down or radio buttons

During the user flow creation, you can change the Page UI customization for the attributes. You can also edit this after creating the user flow by selecting Edit > Page UI customization > Local account sign-up page. This displays the current attributes and how they are collected.

You can click on an attribute to change how it is displayed. You can also indicate that the attributes are not optional.

With these changes, you can execute the user flow and enter the sign-up flow.

Profile Edit User Flow

You will want to create a profile edit user flow with the following settings.

User Flow Section	Settings
Name	GDPR_Sample_ProfileEdit
Identity Providers	• Local Account SignIn
Profile attributes	• emailMarketing • shareDataWithTP
Application claims	• Any claims you want to pass to your app, including any GDPR claims
Page UI customization	Update the Local account sign-up page attributes to use an appropriate input field, either drop down or radio buttons and set the display labels

As with the sign-up user flow, you can edit the labels and input fields for the attributes.

Custom Policies

These custom policies build on the base policy from the SocialAndLocalAccounts policy set available on GitHub.

The extensions policy provides the common elements for the following sign-up and profile edit policies.

For more information on using custom policies, please refer to the documentation.

Extensions Policy (with samples)

This extensions policy contains the common elements required to support the GDPR flow:

- Claims
- Technical Profiles for User Input
- Technical Profiles for reading and writing data to Azure AD B2C User store

The technical profiles to read and write data refer to the attributes that you have created in the section above (Attribute Creation). These are stored in Azure AD B2C in an extensions application which you can view in the Azure Active Directory blade in your Azure AD B2C

tenant. This applications name is "b2c-extensions-app. Do not modify. Used by AADB2C for storing user data.".

Important!

Here, you can see the application Id of the extensions app, which is a GUID. In the policy, you will refer to custom attributes you have created using this notation: "extension_{b2c-extensions-app - Application Id without dashes}_{attribute Name}".

If your extensions app Id is b8ae3b7c-776a-4322-b677-d0900504c1d3, and you are referring to an attribute you named "emailMarketing", the attribute reference would be "extension_b8ae3b7c776a4322b677d0900504c1d3_emailMarketing".

```xml
<?xml version="1.0" encoding="utf-8" ?>
<TrustFrameworkPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="http://schemas.microsoft.com/online/cpim/schemas/2013/06"
  PolicySchemaVersion="0.3.0.0"
  TenantId="yourtenant.onmicrosoft.com"
  PolicyId="B2C_1A_GDPR_Example_TrustFrameworkExtensions"

PublicPolicyUri="http://yourtenant.onmicrosoft.com/B2C_1A_GDPR_Example_TrustFrameworkExtensions"
>

  <!--
    This extensions policy is meant to be applied on top of the base policy from the
    SocialAndLocalAccounts starter pack.

    As with other custom policies, you need to update the following elements:
    - TenantId (change from yourtenant.onmicrosoft.com to your tenant name)
    - The base policy id in the BasePolicy section
    - clientId and IdTokenAudience in the Local Account SignIn section
    - extension attribute app id
      {b2c-extensions-appId-NoDashes} needs to be replaced
      with your extensions app id
  -->

  <BasePolicy>
    <TenantId>yourtenant.onmicrosoft.com</TenantId>
    <PolicyId>B2C_1A_GDPR_Example_TrustFrameworkBase</PolicyId>
  </BasePolicy>

  <BuildingBlocks>

    <ClaimsSchema>
      <!-- These are the claims required for the GDPR experience -->
```

```xml
<ClaimType Id="shareDataWithTP">
  <DisplayName>I consent to allow you to share data with third parties.</DisplayName>
  <DataType>boolean</DataType>
  <DefaultPartnerClaimTypes>
    <Protocol Name="OAuth2" PartnerClaimType="ShareDataWithTP" />
    <Protocol Name="OpenIdConnect" PartnerClaimType="ShareDataWithTP" />
    <Protocol Name="SAML2"

PartnerClaimType="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ShareDataTPConsented" />
  </DefaultPartnerClaimTypes>
  <UserInputType>CheckboxMultiSelect</UserInputType>
  <Restriction>
    <Enumeration Text="" Value="true" SelectByDefault="false" />
  </Restriction>
</ClaimType>

<ClaimType Id="emailMarketing">
  <DisplayName>I consent to allow you to email me marketing information.</DisplayName>
  <DataType>boolean</DataType>
  <DefaultPartnerClaimTypes>
    <Protocol Name="OAuth2" PartnerClaimType="EmailMarketing" />
    <Protocol Name="OpenIdConnect" PartnerClaimType="EmailMarketing" />
    <Protocol Name="SAML2"

PartnerClaimType="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ShareMarketingConsented"
/>
  </DefaultPartnerClaimTypes>
  <UserInputType>CheckboxMultiSelect</UserInputType>
  <Restriction>
    <Enumeration Text="" Value="true" SelectByDefault="false" />
  </Restriction>
</ClaimType>

<ClaimType Id="DOB">
  <DisplayName>Date of Birth</DisplayName>
  <DataType>string</DataType>
  <DefaultPartnerClaimTypes>
    <Protocol Name="OAuth2" PartnerClaimType="DOB" />
    <Protocol Name="OpenIdConnect" PartnerClaimType="DOB" />
    <Protocol Name="SAML2"
PartnerClaimType="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/DOB" />
  </DefaultPartnerClaimTypes>
  <UserHelpText>Date of Birth e.g. 12/21/2000</UserHelpText>
  <UserInputType>TextBox</UserInputType>
</ClaimType>

<ClaimType Id="country">
```

```xml
      <DisplayName>country</DisplayName>
      <DataType>string</DataType>
      <DefaultPartnerClaimTypes>
        <Protocol Name="OAuth2" PartnerClaimType="country" />
        <Protocol Name="OpenIdConnect" PartnerClaimType="country" />
        <Protocol Name="SAML2"
PartnerClaimType="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country" />
      </DefaultPartnerClaimTypes>
      <UserInputType>DropdownSingleSelect</UserInputType>
      <Restriction>
        <Enumeration Text="United Kingdom" Value="United Kingdom" SelectByDefault="false" />
        <Enumeration Text="France" Value="France" SelectByDefault="false" />
        <Enumeration Text="Germany" Value="Germany" SelectByDefault="false" />
      </Restriction>
    </ClaimType>

  </ClaimsSchema>
</BuildingBlocks>

<ClaimsProviders>

  <ClaimsProvider>
    <DisplayName>Local Account SignIn</DisplayName>
    <TechnicalProfiles>
      <TechnicalProfile Id="login-NonInteractive">
        <Metadata>
          <Item Key="client_id">ProxyIdentityExperienceFrameworkAppId</Item>
          <Item Key="IdTokenAudience">IdentityExperienceFrameworkAppId</Item>
        </Metadata>
        <InputClaims>
          <InputClaim ClaimTypeReferenceId="client_id"
            DefaultValue="ProxyIdentityExperienceFrameworkAppId" />
          <InputClaim ClaimTypeReferenceId="resource_id"
            PartnerClaimType="resource" DefaultValue="IdentityExperienceFrameworkAppId" />
        </InputClaims>
      </TechnicalProfile>
    </TechnicalProfiles>
  </ClaimsProvider>

  <ClaimsProvider>
    <DisplayName>Local Account</DisplayName>
    <TechnicalProfiles >

    <!--
        This technical profile includes the output claims required for the GDPR
        sign-in & sign-up experience.

        This adds the elements of country and date of birth, as well as two check
```

```xml
      boxes for sharing data with third parties and email marketing consent.

      All claims must be included here to provide the correct ordering in the Azure B2C UI.
     -->
    <TechnicalProfile Id="LocalAccountSignUpWithLogonEmail">
      <OutputClaims>
        <OutputClaim ClaimTypeReferenceId="objectId" />
        <OutputClaim ClaimTypeReferenceId="email" PartnerClaimType="Verified.Email"
          Required="true" />
        <OutputClaim ClaimTypeReferenceId="newPassword" Required="true" />
        <OutputClaim ClaimTypeReferenceId="reenterPassword" Required="true" />
        <OutputClaim ClaimTypeReferenceId="executed-SelfAsserted-Input"
          DefaultValue="true" />
        <OutputClaim ClaimTypeReferenceId="authenticationSource" />
        <OutputClaim ClaimTypeReferenceId="newUser" />

        <!-- Optional claims, to be collected from the user -->
        <OutputClaim ClaimTypeReferenceId="displayName" />
        <OutputClaim ClaimTypeReferenceId="givenName" />
        <OutputClaim ClaimTypeReferenceId="surName" />

        <OutputClaim ClaimTypeReferenceId="country" Required="true"/>
        <OutputClaim ClaimTypeReferenceId="DOB" Required="true"/>
        <OutputClaim ClaimTypeReferenceId="emailMarketing" DefaultValue="false"/>
        <OutputClaim ClaimTypeReferenceId="shareDataWithTP" DefaultValue="false"/>
      </OutputClaims>
    </TechnicalProfile>

  </TechnicalProfiles>
</ClaimsProvider>

<ClaimsProvider>
  <DisplayName>Self Asserted</DisplayName>
  <TechnicalProfiles>

    <!--
      This technical profile includes the output claims required for the GDPR
      profile edit experience.

      This adds the elements showing and allowing the user to change the consent
      for sharing data and email marketing consent.

      All claims must be included here to provide the correct ordering in the
      Azure B2C UI.
     -->
    <TechnicalProfile Id="SelfAsserted-ProfileUpdate">
      <InputClaims>
        <InputClaim ClaimTypeReferenceId="alternativeSecurityId" />
```

```xml
            <InputClaim ClaimTypeReferenceId="userPrincipalName" />
            <!--
              Optional claims. These claims are collected from the user and can be modified.
              Any claim added here should be updated in the ValidationTechnicalProfile
              referenced below so it can be written to directory after being updateed by
              the user, i.e. AAD-UserWriteProfileUsingObjectId.
            -->
            <InputClaim ClaimTypeReferenceId="givenName" />
            <InputClaim ClaimTypeReferenceId="surname" />
            <InputClaim ClaimTypeReferenceId="emailMarketing" />
            <InputClaim ClaimTypeReferenceId="shareDataWithTP" />
          </InputClaims>
          <OutputClaims>
            <!-- Required claims -->
            <OutputClaim ClaimTypeReferenceId="executed-SelfAsserted-Input"
              DefaultValue="true" />
            <!--
              Optional claims. These claims are collected from the user and can be
              modified. Any claim added here should be updated in the ValidationTechnicalProfile
              referenced below so it can be written to directory after being updateed by the
              user, i.e. AAD-UserWriteProfileUsingObjectId.
            -->
            <OutputClaim ClaimTypeReferenceId="givenName" />
            <OutputClaim ClaimTypeReferenceId="surname" />
            <OutputClaim ClaimTypeReferenceId="emailMarketing" />
            <OutputClaim ClaimTypeReferenceId="shareDataWithTP" />
          </OutputClaims>
        </TechnicalProfile>

      </TechnicalProfiles>
    </ClaimsProvider>

    <ClaimsProvider>
      <DisplayName>Azure Active Directory</DisplayName>
      <TechnicalProfiles>

        <!--
          These Technical Profiles provide the data flow between the different
          elements, defining the storage and output of the GDPR claims for both
          the sign-up and the profile edit user journeys.
        -->

        <TechnicalProfile Id="AAD-Common">
          <Metadata>
            <Item Key="ApplicationObjectId">{b2c-extensions-app - Object Id}</Item>
            <Item Key="ClientId">{b2c-extensions-app - Application Id}</Item>
          </Metadata>
        </TechnicalProfile>
```

```xml
<!--
  The AAD-UserReadUsingObjectId profile is used in the sign-in journey when a
  user already exists, as well as in the edit profile user journey.
-->
<TechnicalProfile Id="AAD-UserReadUsingObjectId">
  <OutputClaims>
    <OutputClaim ClaimTypeReferenceId="emailMarketing"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_emailMarketing" />
    <OutputClaim ClaimTypeReferenceId="shareDataWithTP"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_shareDataWithTP" />
    <OutputClaim ClaimTypeReferenceId="DOB"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_DateOfBirth" />
    <OutputClaim ClaimTypeReferenceId="country" />
  </OutputClaims>
</TechnicalProfile>

<!--
  The AAD-UserWriteUsingLogonEmail profile is used in the sign-up journey when
  a user is created.
-->
<TechnicalProfile Id="AAD-UserWriteUsingLogonEmail">
  <PersistedClaims>
    <PersistedClaim ClaimTypeReferenceId="emailMarketing"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_emailMarketing" />
    <PersistedClaim ClaimTypeReferenceId="shareDataWithTP"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_shareDataWithTP" />
    <PersistedClaim ClaimTypeReferenceId="DOB"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_DateOfBirth" />
    <PersistedClaim ClaimTypeReferenceId="country" />
  </PersistedClaims>
</TechnicalProfile>

<!--
  The AAD-UserWriteProfileUsingObjectId writes changes after profile
  changes have been made
-->
<TechnicalProfile Id="AAD-UserWriteProfileUsingObjectId">
  <PersistedClaims>
    <PersistedClaim ClaimTypeReferenceId="emailMarketing"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_emailMarketing" />
    <PersistedClaim ClaimTypeReferenceId="shareDataWithTP"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_shareDataWithTP" />
    <PersistedClaim ClaimTypeReferenceId="DOB"
      PartnerClaimType="extension_{b2c-extensions-appId-NoDashes}_DateOfBirth" />
    <PersistedClaim ClaimTypeReferenceId="country" />
  </PersistedClaims>
</TechnicalProfile>
```

```xml
      </TechnicalProfiles>
    </ClaimsProvider>
  </ClaimsProviders>
</TrustFrameworkPolicy>
```

Sign-In / Sign-Up Policy (with samples)

The sign-up policy only needs the additional claims that your app requires. Otherwise, the policy is identical to the one in the SocialAndLocalAccounts set.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TrustFrameworkPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="http://schemas.microsoft.com/online/cpim/schemas/2013/06"
  PolicySchemaVersion="0.3.0.0"
  TenantId="yourtenant.onmicrosoft.com"
  PolicyId="B2C_1A_GDPR_Example_signup_signin"
  PublicPolicyUri="http://yourtenant.onmicrosoft.com/B2C_1A_GDPR_Example_signup_signin">

  <BasePolicy>
    <TenantId>yourtenant.onmicrosoft.com</TenantId>
    <PolicyId>B2C_1A_GDPR_Example_TrustFrameworkExtensions</PolicyId>
  </BasePolicy>

  <RelyingParty>
    <DefaultUserJourney ReferenceId="SignUpOrSignIn" />
    <TechnicalProfile Id="PolicyProfile">
      <DisplayName>PolicyProfile</DisplayName>
      <Protocol Name="OpenIdConnect" />
      <OutputClaims>
        <OutputClaim ClaimTypeReferenceId="displayName" />
        <OutputClaim ClaimTypeReferenceId="givenName" />
        <OutputClaim ClaimTypeReferenceId="surname" />
        <OutputClaim ClaimTypeReferenceId="objectId" PartnerClaimType="sub"/>
        <OutputClaim ClaimTypeReferenceId="identityProvider" />
        <OutputClaim ClaimTypeReferenceId="DOB" />
        <OutputClaim ClaimTypeReferenceId="country" />
        <OutputClaim ClaimTypeReferenceId="emailMarketing" />
        <OutputClaim ClaimTypeReferenceId="shareDataWithTP" />
      </OutputClaims>
      <SubjectNamingInfo ClaimType="sub" />
    </TechnicalProfile>
  </RelyingParty>
</TrustFrameworkPolicy>
```

When using the policy, this is the UI displayed when starting the sign-up process. The app then receives a set of claims like the ones on the right.

Verification is necessary. Please click Send button.

Email Address

[Email Address]

[Send verification code]

New Password

[New Password]

Confirm New Password

[Confirm New Password]

Display Name

[Display Name]

Given Name

[Given Name]

Surname

[Surname]

country

[country ▼]

Date of Birth

[Date of Birth]

☐ I consent to allow you to email me marketing information.

☐ I consent to allow you to share data with third parties.

[Create] [Cancel]

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "IvWUjf-sgFD6rC-eqC8z3Lx1y2sgIC2UnB6lWOaJ6FQ"
}.{
  "exp": 1535060286,
  "nbf": 1535056686,
  "ver": "1.0",
  "iss": "https://login.microsoftonline.com/.../v2.0/",
  "sub": "...",
  "aud": "...",
  "acr": "b2c_1a_gdpr_test_signup_signin",
  "nonce": "defaultNonce",
  "iat": 1535056686,
  "auth_time": 1535056686,
  "name": "TestUser",
  "given_name": "Test",
  "family_name": "User",
  "country": "France",
  "DOB": "01/01/1980",
  "EmailMarketing": false,
  "ShareDataWithTP": false
}.[Signature]
```

Profile Edit Policy (with samples)

The profile edit policy only needs the additional claims that your app requires. Otherwise, the policy is identical to the one in the SocialAndLocalAccounts set. You will likely want to provide the same set of claims to the application as the sign-in/sign-up policy.

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TrustFrameworkPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="http://schemas.microsoft.com/online/cpim/schemas/2013/06"
  PolicySchemaVersion="0.3.0.0"
  TenantId="yourtenant.onmicrosoft.com"
  PolicyId="B2C_1A_GDPR_Example_ProfileEdit"
  PublicPolicyUri="http://yourtenant.onmicrosoft.com/B2C_1A_GDPR_Example_ProfileEdit">

  <BasePolicy>
    <TenantId>yourtenant.onmicrosoft.com</TenantId>
    <PolicyId>B2C_1A_GDPR_Example_TrustFrameworkExtensions</PolicyId>
  </BasePolicy>

  <RelyingParty>
    <DefaultUserJourney ReferenceId="ProfileEdit" />
```

```xml
<TechnicalProfile Id="PolicyProfile">
  <DisplayName>PolicyProfile</DisplayName>
  <Protocol Name="OpenIdConnect" />
  <OutputClaims>
    <OutputClaim ClaimTypeReferenceId="displayName" />
    <OutputClaim ClaimTypeReferenceId="givenName" />
    <OutputClaim ClaimTypeReferenceId="surname" />
    <OutputClaim ClaimTypeReferenceId="objectId" PartnerClaimType="sub"/>
    <OutputClaim ClaimTypeReferenceId="identityProvider" />
    <OutputClaim ClaimTypeReferenceId="DOB" />
    <OutputClaim ClaimTypeReferenceId="country" />
    <OutputClaim ClaimTypeReferenceId="emailMarketing" />
    <OutputClaim ClaimTypeReferenceId="shareDataWithTP" />
  </OutputClaims>
  <SubjectNamingInfo ClaimType="sub" />
</TechnicalProfile>
    </RelyingParty>
</TrustFrameworkPolicy>
```

Given Name

Given Name

Surname

Surname

I consent to allow you to email me marketing information.
☐

I consent to allow you to share data with third parties.
☐

[Continue] [Cancel]

Developer Guidance – Graph API

The Graph API is a programmatic interface to read, change, and delete data contained within the Azure AD B2C directory. Azure AD B2C tenants tend to be very large. This means that many common tenant management tasks need to be performed programmatically. A primary example is user management.

Permissions

The documentation for using the Graph API with Azure AD B2C shows how to enable the proper permissions to interact with the directory. There are specific actions which require additional permissions:

- Currently, the read and write directory data permission does not include the ability to do any deletions such as deleting users. The documentation has specific instructions to enable permissions for an app to perform delete actions

Read Actions

You can read users individually or as a group. To read all users from the directory, call the users method without an objectId specified. The result output is truncated for brevity.

```
GET: https://graph.windows.net/yourtenant.onmicrosoft.com/users?api-version=1.6
```

```
{
    "odata.metadata":
"https://graph.windows.net/yourtenant.onmicrosoft.com/$metadata#directoryObjects/Micro
soft.DirectoryServices.User",
    "value": [
        {
            "odata.type": "Microsoft.DirectoryServices.User",
            "objectType": "User",
            "objectId": "3ca1aad0-85ce-491a-a1f8-27646fef2b1e",
            ...
            "userStateChangedOn": null,
            "userType": "Member",
            "extension_3b5b47dc8fc94097bf9eca4f73081786_emailMarketing": true
        },
        {
            "odata.type": "Microsoft.DirectoryServices.User",
            "objectType": "User",
            "objectId": "579ef843-707a-4f36-93f0-82141ef8b372",
            ...
            "userStateChangedOn": null,
            "userType": "Member",
            "extension_3b5b47dc8fc94097bf9eca4f73081786_emailMarketing": false
        }
    ]
}
```

To read an individual user, specify the objectId of the user in the url. The result output is truncated for brevity.

```
GET: https://graph.windows.net/yourtenant.onmicrosoft.com/users/3ca1aad0-85ce-491a-
a1f8-27646fef2b1e?api-version=1.6
```

```
{
    "odata.metadata":
"https://graph.windows.net/yourtenant.onmicrosoft.com/$metadata#directoryObjects/Micro
soft.DirectoryServices.User/@Element",
    "odata.type": "Microsoft.DirectoryServices.User",
    "objectType": "User",
    "objectId": "3ca1aad0-85ce-491a-a1f8-27646fef2b1e ",
    ...
    "userPrincipalName": "725906aa-5caa-48c1-9180-
1dc4965ce2e7@yourtenant.onmicrosoft.com",
    "userState": null,
    "userStateChangedOn": null,
    "userType": "Member"
}
```

Write Actions

Write actions include creating new users or updating existing users. You can create a new user using a Post action. The result output is truncated for brevity.

```
POST: https://graph.windows.net/yourtenant.onmicrosoft.com/users?api-version=1.6

{
    "accountEnabled": true,
    "signInNames": [
        {
            "type": "emailAddress",
            "value": "username@gmail.com"
        }
    ],
    "creationType": "LocalAccount",
    "displayName": "User Name",
    "mailNickname": "user",
    "passwordProfile": {
        "password": "P@ssword!",
        "forceChangePasswordNextLogin": false
    },
    "passwordPolicies": "DisablePasswordExpiration"
}
```

```
{
    "odata.metadata":
"https://graph.windows.net/yourtenant.onmicrosoft.com/$metadata#directoryObjects/Micro
soft.DirectoryServices.User/@Element",
    "odata.type": "Microsoft.DirectoryServices.User",
    "objectType": "User",
    "objectId": "3ca1aad0-85ce-491a-a1f8-27646fef2b1e",
    ...
    "userState": null,
    "userStateChangedOn": null,
    "userType": "Member"
}
```

You can also update an existing user by specifying the objectId of the user in a Patch action. There is no response object from the Patch action.

```
PATCH: https://graph.windows.net/yourtenant.onmicrosoft.com/users/c037e435-a279-4c72-
99a6-6721404c4010?api-version=1.6

{
    "extension_3b5b47dc8fc94097bf9eca4f73081786_emailMarketing": false
}
```

Delete Actions

To delete a user and all data associated with the user, send a Delete action including the objectId of the user to delete. As discussed in the permissions section, delete requests require additional permissions than the standard read & write permissions. There is no response object from the Delete action.

```
DELETE: https://graph.windows.net/yourtenant.onmicrosoft.com/users/c037e435-a279-4c72-
99a6-6721404c4010?api-version=1.6
```

Solution Support and Analytics

Getting support from Microsoft

Azure Support: Depending on your Enterprise Agreement with Microsoft, you can call Microsoft Support and open a ticket for any issue related to your Azure Identity deployment. For more information on how to get in touch with Microsoft Support, please visit our Azure support portal: https://azure.microsoft.com/support

FastTrack: If you have purchased Enterprise Mobility and Security (EMS) licenses or Azure AD Premium licenses, you may be eligible to receive deployment assistance from the FastTrack program. For more information on how to engage with FastTrack, please refer to our documentation on the FastTrack Center Eligibility Benefit for Enterprise Mobility and Security

Engage the Product Engineering Team: If you are working on a major customer deployment with millions of users, you can work with your Microsoft account team or your Cloud Solutions Architect to decide if the project's deployment complexity warrants working directly with the Azure Identity Product Engineering team.

EMS Blog: Subscribe to the EMS Blog to stay up to date with all the latest product announcements, deep dives, and roadmap information provided directly by the Identity engineering team. You can also post comments and get feedback from the engineering group.

Azure Active Directory Public Forums: Azure AD also has several closely monitored channels available to the public. Here are some useful links:

- Stack Overflow using the tag 'azure-ad-b2c'
- MSDN Forum for Azure AD
- UserVoice to submit or vote on new feature requests in Azure AD B2C

Code Samples on GitHub:

- Azure AD B2C

Additional Resources

- Microsoft Azure Active Directory B2C Solution Guides
- How Microsoft Azure Can Help Organizations Become Compliant with the EU General Data Protection Regulation
- Gaining Expertise with Azure AD B2C: A course for developers
- Azure Active Directory B2C code samples