Ascent360
MEET YOUR DATA

Email Permission Management

This article describes how our email permission system works. Determining email permission is a complex process that leverages all available data to determine the correct email permission for each person in your database. Our goal is to ensure that our clients have the tools to properly follow rules and regulations -- including the various permutations of CASL, GDPR, and CAN-SPAM.

In this article:

Fields that Help Inform Email Permission

Field	Definition
SPAM Law Authority	Each individual email address in our system is governed by a specific SPAM Law. Currently, this can be CASL, CAN-SPAM and GDPR. The specific SPAM Law authority will help define how the individual email address is treated in our system.
Email Permission	Email Permission is set to either “Yes” or “No”. If email permission is set to “No,” it is not possible to send the contact an email in Ascent360 or send the contact to an external Email Service Provider (ESP). Email Permission is the final result of all the logic to define if an individual is contactable.
Email Permission Status	Email Permission Status is similar to email permission but is more granular and can be set to “Yes”, “No” or “Unknown”. • “Yes” means that we have explicit permission from the individual that says, “I would like to hear from your company via email”. “Yes” is a hard opt in and qualifies for GDPR explicit status. • “No” means that we have an explicit Opt-Out. This is often from an email service provider such as Ascent360 or Acoustic, but it can also come from a source system such as an eCommerce system that collects and stores explicit opt outs. • “Unknown” means that we have neither an explicit No or an explicit Yes. This is often referred to as “implied consent” since the consumer gave us their email address through a transaction. A transaction is defined as an interaction with the customer’s company and can be a variety of things including a purchase or a web form completion.

Source (Source Type)	100% of the records that are loaded into the Ascent360 platform require a source to identify where the data originated. This could say “MailChimp” if the data is coming from MailChimp or it could say “Web Form XYZ” if the data is coming from a form on a website. This is meaningful for email permissions because if we get a “Hard Opt In” (explicit yes), then we want to be able to track when and where we received that hard opt in. At some point in the future, if you get a complaint from a consumer that says, “Why did I get an email? I never opted in.”, Ascent360 will be able to tell you that the individual really did opt in on a specific date and from what source.
Source Date (List Source Date)	Source Date is the date related to the source of the data. This is typically the date we received the record. However, the date may also be years old. As an example, if we are loading data from a legacy eCommerce system and many transactions occurred years ago, then we will use the transaction date, or an explicit email subscribe date if there is one.
Email Domain Extension	The extension of the email address often signifies the country in which the owner of the domain lives. Ascent360 uses the email domain extension as one dimension to inform the correct SPAM Law Authority of the individual. ICAAN, the regulatory body in charge of the internet addressing system has created a domain extension for all countries in the world as well as some regions. As an example, there is a .UK extension to signify the United Kingdom and a .EU to signify the European Union. It must be noted that it is not actually necessary to live in the EU to have a .EU extension. It is possible simply to sign up for a .EU extension. For this reason, Ascent360 will prioritize a physical address over a domain extension.
Country Code	If Ascent360 receives any physical address data from any of the incoming data sources, we will attempt to define what Country the address is in. Ascent360 uses third party data sources, such as the US Postal Service database to add the country code. We do not use IP address or any Geo Location to define the country and we do not plan on doing this in the future as we do not believe this is an accurate way to assume physical location. Ascent360 does add an ISO standard country code to the system.
Client Country	Our clients are located or headquartered in various countries. Many are headquartered in the United States or Canada. The clients’ country does change how Ascent360 determines the rules by which we manage our clients’ data. If the client country is Canada, we will assume that individuals with no physical address or domain country extension are located in Canada. However, if our client is located in the United States, we will assume that individuals with no physical address data or domain country extension are located in the United States.
Last Transaction Date	Last Transaction Date is a date set for each individual that notes the last date on which they made a financial purchase. This is important for determining implied status in CASL Regulations.
Source Opt Status	Source Opt Status is the “Email Permission Status” that came from the source. Source Opt Status essentially asks the question, was the intent of the individual who put their email address into the system an Explicit Opt In, an Explicit Opt Out, or is that not known.

SPAM Law Authority

Ascent360 determines what SPAM Law Authority should apply to a person in our database based upon two fields. These are “Country Code” and “Email Domain Extension”.

Ascent360 will map an individual email address to the email domain extension based upon the country code of origin. If an individual is physically located in France, then Ascent360 will assign the SPAM Law Authority of GDPR. This is regardless of what email domain extension they have. As you can see below, even if the person has a .ca(Canadian) domain extension but their physical address is in France, we will assign the SPAM Law Authority of

GDPR per the law of France. Many people who live all over the world use a .com extension. We will again default to their country of their physical address.

If the country of the physical address is blank, we will use the email domain extension. So, if the physical address country is unknown, but the email domain extension is .ca, we will assign the SPAM Law Authority of CASL per the law of Canada. Rather, if the extension is .fr (France) we will assign SPAM Law Authority of GDPR.

Example SPAM Law Authority Assignment Based upon Country Code and Email Domain Extension

		Country Code (Primary)						
		AUT	**BEL**	**CAN**	**DEU**	**FRA**	**USA**	**Unknown**
Email Domain Extension (Secondary)	**.at**	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	GDPR
	.au	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	CAN-SPAM
	.biz	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	CAN-SPAM
	.ca	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	CASL
	.co	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	CAN-SPAM
	.com	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	CAN-SPAM
	.de	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	GDPR
	.fr	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	GDPR
	.uk	GDPR	GDPR	CASL	GDPR	GDPR	CAN-SPAM	GDPR

Client Country Identification

If a client identifies as a US company, individuals with an unknown (implied) email permission status will have the “Email Permission” set to Yes. However, if our client defines themselves as being an EU company, a person with an unknown (implied) email permission status will have the “Email Permission” set to No.

Simply stated, if our client is in Canada, all unknowns follow CASL Regulations. If the client is in the EU or the UK, all Unknowns follow GDPR regulations and if our client is in some other country, unknowns will follow CAN-SPAM regulations.

Any of our clients can choose which of the three paths to follow. So even if our client is headquartered in Michigan, they can choose to follow the Canadian Identification and CASL regulation path.

Email Permission Status

Ascent360 will set the “Email Permission Status” field based upon our understanding of the intent of the individual through the source system from which we have received their data. Some systems, like Springer Miller Systems, include an “Explicit Opt-Out” field which we will use to add a hard opt-out to the record. Springer Miller Systems does not have an “Explicit Opt-In” field, so every record that comes in to our system that does not have a hard opt-out will be marked with an “Unknown” or “Implied” opt in. This does not necessarily mean that we can communicate with the individual as CASL or GDPR laws may exclude us from doing so.

100% of the records that come in with an email address will be marked as either Yes, No or Unknown (Explicit Yes, Explicit No or Implied). Ascent360 will also tag the source of the record and the date of the source.

Multiple Sources of Opt-In Data

Many of the individuals in our solution will come from multiple sources. Individuals records may show an explicit opt-out, explicit opt-in or implied opt-in. Ascent360 will merge these sources and only use the most recent explicit yes or explicit no. This means that an explicit yes that comes in AFTER an explicit no will override the explicit no. Similarly, an explicit no that comes in after an explicit yes will also override the explicit yes.

An implied or unknown cannot override an explicit yes or an explicit no.

Ascent360 saves 100% of the records that we are sent by all source systems. This means that the email permission status will be based upon the entire history of data from all sources. As noted above, an individual may enter the database with implied permission, may then opt out, and may then opt back in.

Final Email Permission

As noted in the definitions, Ascent360 has a field called “Email Permission” which is the final authority to determine if we are able to communicate with an individual via email.   This field is set to either Yes or No.   If the field is set to No, our system will not allow you to send email to the individual.

The table below shows all the permutations of Client Country, SPAM Law Authority, Email Permission Status, and Transaction Past 23 Months which then fully identifies what the Final Email Permission should be.

Client Country	SPAM Law Authority	Email Permission Status	Transaction Past 23 Months?	Email Permission
Client Identifies as Canadian Company	CAN-SPAM	Explicit No	n/a	**No**
Client Identifies as Canadian Company	CAN-SPAM	Explicit Yes	n/a	**Yes**
Client Identifies as Canadian Company	CAN-SPAM	Implied	No	**No**
Client Identifies as Canadian Company	CAN-SPAM	Implied	Yes	**Yes**
Client Identifies as Canadian Company	CASL	Explicit No	n/a	**No**

Client Identifies as Canadian Company	CASL	Explicit Yes	n/a	**Yes**
Client Identifies as Canadian Company	CASL	Implied	No	**No**
Client Identifies as Canadian Company	CASL	Implied	Yes	**Yes**
Client Identifies as Canadian Company	GDPR	Explicit No	n/a	**No**
Client Identifies as Canadian Company	GDPR	Explicit Yes	n/a	**Yes**
Client Identifies as Canadian Company	GDPR	Implied	No	**No**
Client Identifies as Canadian Company	GDPR	Implied	Yes	**No**
Client identifies as EU Company	CAN-SPAM	Explicit No	n/a	**No**
Client identifies as EU Company	CAN-SPAM	Explicit Yes	n/a	**Yes**
Client identifies as EU Company	CAN-SPAM	Implied	n/a	**No**
Client identifies as EU Company	CASL	Explicit No	n/a	**No**
Client identifies as EU Company	CASL	Explicit Yes	n/a	**Yes**
Client identifies as EU Company	CASL	Implied	No	**No**
Client identifies as EU Company	CASL	Implied	Yes	**Yes**
Client identifies as EU Company	GDPR	Explicit No	n/a	**No**
Client identifies as EU Company	GDPR	Explicit Yes	n/a	**Yes**
Client identifies as EU Company	GDPR	Implied	n/a	**Yes**
Client Identifies as Non EU / Canada Company	CAN-SPAM	Explicit No	n/a	**No**
Client Identifies as Non EU / Canada Company	CAN-SPAM	Explicit Yes	n/a	**Yes**
Client Identifies as Non EU / Canada Company	CAN-SPAM	Implied	n/a	**Yes**
Client Identifies as Non EU / Canada Company	CASL	Explicit No	n/a	**No**
Client Identifies as Non EU / Canada Company	CASL	Explicit Yes	n/a	**Yes**
Client Identifies as Non EU / Canada Company	CASL	Implied	No	**No**
Client Identifies as Non EU / Canada Company	CASL	Implied	Yes	**Yes**
Client Identifies as Non EU / Canada Company	GDPR	Explicit No	n/a	**No**
Client Identifies as Non EU / Canada Company	GDPR	Explicit Yes	n/a	**Yes**
Client Identifies as Non EU / Canada Company	GDPR	Implied	n/a	**No**

Appendix A: Email Domain Extensions

Appendix A is a list of email Domain Extensions and which SPAM Law Authority they are associated with. Appendix B is a list of country codes and which SPAM Law Authority they are associated with. Please remember that a Country Code will override an Email Domain Extension.

EU	Country	SPAM Law Authority
Austria	.at	GDPR
Belgium	.be	GDPR
Bulgaria	.bg	GDPR
Croatia	.hr	GDPR
Republic of Cyprus	.cy	GDPR
Czech Republic	.cz	GDPR
Denmark	.dk	GDPR
Estonia	.ee	GDPR
Finland	.fi	GDPR
France	.fr	GDPR
Germany	.de	GDPR
Greece	.gr	GDPR
Hungary	.hu	GDPR
Ireland	.ie	GDPR
Italy	.it	GDPR
Latvia	.lv	GDPR
Lithuania	.lt	GDPR
Luxembourg	.lu	GDPR
Malta	.mt	GDPR
Netherlands	.nl	GDPR
Poland	.pl	GDPR
Portugal	.pt	GDPR
Romania	.ro	GDPR
Slovakia	.sk	GDPR
Slovenia	.si	GDPR

Spain	.es	GDPR
Sweden	.se	GDPR
United Kingdom	.uk	GDPR
Europe	.eu	GDPR
Canada	.ca	CASL
Unknown	.com	CAN-SPAM
Unknown	.net	CAN-SPAM
Unknown	.org	CAN-SPAM
All Others	.XXX	CAN-SPAM

Appendix B: Country Codes

ISO Country Code	Country Name	SPAM Law Authority
AUT	Austria	GDPR
BEL	Belgium	GDPR
BGR	Bulgaria	GDPR
HRV	Croatia	GDPR
CYP	Cyprus	GDPR
CZE	Czech Republic	GDPR
DNK	Denmark	GDPR
EST	Estonia	GDPR
FIN	Finland	GDPR
FRA	France	GDPR
DEU	Germany	GDPR
GRC	Greece	GDPR
HUN	Hungary	GDPR
IRL	Ireland	GDPR
ITA	Italy	GDPR

LVA	Latvia	GDPR
LTU	Lithuania	GDPR
LUX	Luxembourg	GDPR
MLT	Malta	GDPR
NLD	Netherlands	GDPR
POL	Poland	GDPR
PRT	Portugal	GDPR
ROU	Romania	GDPR
SVK	Slovakia	GDPR
SVN	Slovenia	GDPR
ESP	Spain	GDPR
SWE	Sweden	GDPR
GBR	United Kingdom	GDPR
CAN	Canada	CASL
USA	United States	CAN-SPAM
XXX	All Others	CAN-SPAM