	Privacy Regulation	Jurisdiction	What Is it?	How & What Consent Obtained	Product Level Notifications
1.a	General Data Protection Regulation (**GDPR**) 2018	Europe	Wide-ranging and comprehensive regulation to better protect the privacy of European citizens and provide them with more control over their own personal information (PI) or data.	**Explicit Consent:** Must ask subjects, for permission on use of PI. This permission can no longer be 'implicit' (for instance, by pre-ticked options), but must be discrete and explicit **'opt-in'** for each contact type - product news, invitations, promos, urgent messages, press releases (for instance, by ticking off an option or an agree button). **NO bundling** of permissions (per Recital 43) allowed - enter contest does not permit future marketing blasts. **Nota:** asking for consent to contact is deemed marketing and is in breach of the GDPR regulations.	**Implied Consent: for contacting and engaging existing customers** via various communications channels is understood to be covered by Legitimate Interest **as defined** in GDPR: this could include bug fix notifications, recalls, release info, product obsolescence/EoL/EoS, update requirements, service advisories, training,etc. Loosely interpreted, also allows 'marketing' type messaging. But, it is preferable to get explicit consent and provide customers with an '**opt-out**' option.
1.b	General Data Protection Regulation (**GDPR-UK**) 2021	U.K.	**Builds on EU-GDPR**. The Data Protection Act 2018 will apply as supplementary legislation to GDPR.	**Explicit Consent:** This is the same as the existing GDPR requirement. **Note:** the updated Data Protection 2018 Act will supplement GDPR once Brexit takes effect.	Same as existing GDPR implications noted above. UK Regulator (ICO) specifically states that for '**soft opt-ins**': means you ***may*** be able to email or text your own customers for a wider range of reasons, but this ability excludes prospective customers or new contacts (i.e. bought lists). Must always offer '**opt-out**' and timely response.
2.	Controlling the Assault of Non-Solicited Pornography and Marketing Act (**CAN-SPAM**) 2003	America	CAN-SPAM doesn't require prior consent from recipients in order to be sent commercial messages.	**Implied Consent:** automatically allows companys to proactively include all desired contacts in their campaigns. This regulatory system follows an **"opt-out"** approach**.** But, it only applies to CEMM - commercial electronic mail messages i.e. specifically only email.	**Implied Consent:** for transactional messages. i.e. in support of a commercial transaction the recipient already has agreed to; gives warranty, recall, safety, or security information; advises of changes to contract terms or features for ongoing commercial relationship. **Mix of Commercial and Transactional Content**: the primary purpose of the message is the deciding factor. If subject line leads recipient to think it's a commercial message, it's a commercial message. If the bulk of the transactional messaging doesn't appear at the beginning, it's a commercial message and must be consented to. Must allow '**opt-out**' in timely manner.
3.	Canadian Anti-Spam Law (**CASL**) 2014	Canada	CASL covers all messages sent into or out of Canada, but excludes messages simply routed through Canada.	**Explicit Consent:** not implicit or inferred and is specifically an '**opt-in**' model, applies to CEM - commercial electronic messages includes text, sound, voice or image messages, and extends to social media messages such as LinkedIn or Facebook. **Note :** cannot 'toggle' for consent, each item requires a separate permission. Org must then provide confirmation. i.e. as with GDPR, cannot tie requests together.	**Implied Consent: CASL** governs **transactional emails**. Must have an unsubscribe or preference page link from which recipients can unsubscribe from promotional **emails**. And if the **transactional email** contains any marketing or promotional content, then it becomes a marketing message and falls under **CASL** regulation, requiring **explicit consent** via '**opt-in**'. **Regardless of Consent on file:** whether Explicit or Implicit, if a recipient asks to stop receiving CEMs through your unsubscribe mechanism or by another form of communication, you must respect their request and stop sending them CEMs within 10 business days
4.a	California Consumer Protection Act (**CCPA**) 2020	California*	Similar to CAN-SPAM, doesn't require prior consent from recipients. Cross-sector legislation which proects individual consumer rights and restricts collection of personal information about, or from, a California resident.	**Implied Consent:** Co's must inform data subjects when and how data is collected, give them the ability to access, correct, delete or **'opt-out'** of providing info. Must be disclosed in a privacy policy displayed on the entity's website that collects the data.	As this regulation is based on **'opt-out'** there are no current items that are deemed to be exceptions - i.e. all types of notifications are allowed.
4.b	California Privacy Rights Act (**CPRA**) 2023	California*	**Builds on CCPA.** Full requirements in place by January 1, 2023.	**Implied Consent: Adds to CCPA requirements noted above** with more GDPR-like right to correct personal information that is inaccurate, along with an **'opt-out'** of both uses and disclosures for a new category of sensitive data, including location data, which are not necessary for the service provided.	See above.

Exceptions	Consent Evidentiary Requirements	Penalties for Breach	Notes of Interest / Resources
Referals from a friend i.e. to claim an offer. The company sends an email to a referred person (net new contact) and per GDPR that is deemed a notification. The mail cannot be stored or processed. Then the referred person must '**opt-in**' to be contacted anytime thereafter. **Push** messages and website **pop-ups** (deemed freely given consent) are allowed as they do not use the person's email.	Must maintain a "data register" that demontrates that a data subject gave permission, and is easily viewable/proveable. Must provide an easy way (quick) to withdraw permission, without unnecessary or time-consuming actions. i.e. unsubscribe link in every email or newsletter, option to update data via the website.	**Variable:** National authorities can assess fines that are effective, proportionate, deterrent on a case by case basis. These fines are uncapped, the higher of €20 million or 4% of the worldwide annual turnover. British Airways (2019) was handed a £183.4m penalty; Marriott International incurred a £99m fine.	1.EU GDPR: **https://ec.europa.eu/justice/smedataprotect/index_en.htm** **Recommended supplementary actions:** Implement an information security management system (ISMS) including policies and measures concerning data protection, of which personal data are a part. A good reference is: **ISO27001** 2.Legitimate Interest: per GDPR - same interpretation used by ICO - see website refererenced
See above.	Same as existing GDPR requirements	**Variable:** UK Regulators will assess fines on a case by case basis, and are capped at £500,000. The Information Commissioners Office (ICO) recently applied these penalites: DSG Retail Ltd (2020) was fined £500,000; Doorstep Dispensaree Ltd 2019) was fined £275,000	1.General Reference Resource from Zivver - 2020: **UK_book_GDPR_Checklist_V1.pdf** 2.ICO Guidelines for Legitimate Use: **https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/**
With a lack of specific details found, it is presumed that there are currently implied exceptions for text, sound, voice or image messages including social media platforms such as LinkedIn or Facebook.	Must maintain a data registry that is easily accessible if audited. Must also provide an easy way to withdraw permission, without delaying actions. Must be 'opted out' within **10** days.	**Variable:** Administrative actions by the Federal Trade Commission includes Administrative Orders, injunctions or prosecution. Civil or Criminal actions are uncapped including statutory damages $1-2M plus aggravated damages. Criminal charges relating to fraudulent acts or spamming up to 5 years and forfeiture of assets. Spammer Christopher William Smith (2006) was fined $5.3 million.	1.Refer to Federal Trade Commission website: **https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business** Note: All comms require a clear and valid postal address of sender along with tel# with vm. 2.CAN-SPAM Requirements - **Salesforce Help Article**.
Existing Business Relationship provides an exception based on **Implied Consent** - based on business related activity within a 2 year period before the communications are sent, or if the customer has made an inquiry of the company within the previous 6 months. **Note:** as with GDPR, cannot tie requests together.	Data registry must be maintained and info easily provided and auditable. Must be 'opted out' within **10** days.	**Variable:** Maximum penalty capped at $1M CDN per violation in case of an individual (including Directors, officers, agents or mandataries), and capped at $10M CDN per violation for a company. Recent penalites include Compu.Finder $1.1M; Rogers Communications $200K Cdn; Porter Airlines $150K. Personal Fine: $100,000 penalty on Mr. Brian Conley for violations committed by nCrowd.	1.Refer to Canadian Government website: **https://crtc.gc.ca/eng/internet/anti.htm** **Note:** All comms require a clear and valid postal address of sender along with tel# with vm or email or web address. _____ 2.Legal Opinion: **https://www.tlrlaw.ca/blog/casl-fines-obligations-consent#**
As this regulation is based on **'opt-out'** there are no current items that are deemed to be exceptions - i.e. all types of notifications are allowed.	Data registry must be maintained and info easily provided and auditable. Must be 'opted out' within **15** days. Information gathered must be properly categorized and managed and accessible for audit. Requires Co's to have a "Do Not Sell my Personal Info" link on website, otherwise info can be gathered.	**Variable:** The CCPA penalities: $2,500 per violation, tripling to $7,500 per intentional violation. Uncapped. Definition of violations are being finalized however, most likely to be applied per consumer affected. First Class Action filed against Salesforce (022020).	Refer to State of California Department of Justice: **https://oag.ca.gov/privacy/ccpa**
See above.	**In addition to CCPA requirements above**, adds a right to 'opt-out' of company's use of profiling technologies. 'Opt-out' also specifically extends to sharing of Personal Info (PI) for cross-context behavioral advertising i.e. " recommendations "	**Variable:** Increases fines to $7,500 for each violation of CPRA involving personal information of consumers under the age of 16. Uncapped. Eliminates the 30-day period following notice that enabled organization to rectify the problem.	**Interesting to note:** "It clearly closes a couple of areas where big companies like Google and Facebook are continuing to track users and collect data," he said. "If you look at some of the previous investigations, Facebook and Google collect most of their data as third parties on other people's properties, so this limits that." **Result - forcing change to 3rd-party cookies**