

CCPA and GDPR Comparison Chart

LAURA JEHL AND ALAN FRIEL, BAKERHOSTETLER LLP,
WITH PRACTICAL LAW DATA PRIVACY ADVISOR

Search the [Resource ID numbers in blue](#) on Westlaw for more.

A Chart comparing some of the key requirements of the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR).

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) took effect on May 25, 2018 and replaced the EU Directive and its member state implementing laws. On June 28, 2018, California became the first U.S. state with a comprehensive consumer privacy law when it enacted the California Consumer Privacy Act of 2018 (CCPA), which becomes effective January 1, 2020, with some exceptions (Cal. Civ. Code §§ 1798.100-1798.199). Given their comprehensiveness and broad reaches, each law may have significant impact on entities that collect and process personal data.

The CCPA grants California resident’s new rights regarding their personal information and imposes various data protection duties on certain entities conducting business in California. While it incorporates several GDPR concepts, such as the rights of access, portability, and data deletion, there are several areas where the CCPA requirements are more specific than those of the GDPR or where the GDPR goes beyond the CCPA requirements.

This Chart provides a high-level comparison of key requirements under the CCPA and the GDPR. It is not a comprehensive list of all measures required under the CCPA or the GDPR.

For an overview of the CCPA, see Practice Note, California Privacy and Data Security Law: Overview: General Data Protection and the California Consumer Privacy Act ([6-597-4106](#)) and Article, Expert Q&A: The California Consumer Privacy Act of 2018 (CCPA) ([W-015-6908](#)).

For an overview of the GDPR, see Practice Note, Overview of EU General Data Protection Regulation ([W-007-9580](#)).

	CCPA	GDPR	Comparison	Practical Law Resources and Citations
Who is Regulated?	<p>Any for-profit entity doing business in California, that meets one of the following:</p> <ul style="list-style-type: none"> ■ Has a gross revenue greater than \$25 million. ■ Annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes. ■ Derives 50 percent or more of its annual revenues from selling consumers’ personal information. <p>The law also applies to any entity that either:</p> <ul style="list-style-type: none"> ■ Controls or is controlled by a covered business. ■ Shares common branding with a covered business, such as a shared name, service mark, or trademark. 	<p>Data controllers and data processors:</p> <ul style="list-style-type: none"> ■ Established in the EU that process personal data in the context of activities of the EU establishment, regardless of whether the data processing takes place within the EU. ■ Not established in the EU that process EU data subjects’ personal data in connection with offering goods or services in the EU, or monitoring their behavior. 	<p>The scope and territorial reach of the GDPR is much broader.</p> <p>Substantially different in parties regulated.</p>	<p>CCPA</p> <p>Cal. Civ. Code § 1798.140(c).</p> <p>Boxes, CCPA Definitions and CCPA Exceptions to Extraterritorial Applications.</p> <p>Practice Note, California Privacy and Data Security Law: Overview: CCPA Scope (6-597-4106).</p> <p>GDPR</p> <p>Article 3.</p> <ul style="list-style-type: none"> ■ Practice Note, Determining the Applicability of the GDPR (W-003-8899).

	CCPA	GDPR	Comparison	Practical Law Resources and Citations
	<p>Parts of the CCPA apply specifically to:</p> <ul style="list-style-type: none"> ■ Service providers. ■ Third parties. 			
Who is Protected?	<p>Consumers, defined as California residents that are either:</p> <ul style="list-style-type: none"> ■ In California for other than a temporary or transitory purpose. ■ Domiciled in California but are currently outside the State for a temporary or transitory purpose. <p>Consumers include:</p> <ul style="list-style-type: none"> ■ Customers of household goods and services. ■ Employees. ■ Business-to-Business transactions. 	<p>Data subjects, defined as identified or identifiable persons to which personal data relates.</p>	<p>Substantially different in approach, but similarly broad in effect.</p> <p>Both laws focus on information that relates to an identifiable natural person, however the definitions differ.</p> <p>Both have potential extraterritorial effects that businesses located outside the jurisdiction must consider.</p>	<p>CCPA</p> <p>Cal. Civ. Code § 1798.140(g) and Cal. Code Regs. tit. 18, §17014.</p> <p>Practice Note, California Privacy and Data Security Law: Overview: CCPA Scope (6-597-4106).</p> <p>GDPR</p> <p>Article 4(1).</p> <p>Practice Note, Overview of EU General Data Protection Regulation: Identifiability (W-007-9580).</p>
What Information is Protected?	<p>Personal information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household.</p> <p>The statutory definition includes a list of specific categories of personal information.</p> <p>Personal information does not include certain publicly available government records. The CCPA also excludes certain personal information covered by other sector specific legislation from its coverage scope.</p>	<p>Personal data is any information relating to an identified or identifiable data subject.</p> <p>The GDPR prohibits processing of defined special categories of personal data unless a lawful justification for processing applies.</p>	<p>Substantially similar. However, the CCPA definition also includes information linked at the household or device level.</p>	<p>CCPA</p> <p>Cal. Civ. Code §§ 1798.140(o) and 1798.145(c)-(f).</p> <p>Boxes, Categories of Personal Information Under the CCPA and Information Excluded From the CCPA's Personal Information Definition.</p> <p>Practice Note, California Privacy and Data Security Law: Overview: Personal Information under CCPA (6-597-4106).</p> <p>GDPR</p> <p>Articles 4(1) and 9(1).</p> <p>Practice Note, Overview of EU General Data Protection Regulation: Personal Data and Data Subjects (W-007-9580) and Special Categories of Personal Data (W-007-9580).</p>
Anonymous, Deidentified, Pseudonymous, or Aggregated Data	<p>The CCPA does not restrict a business's ability to collect, use, retain, sell, or disclose a consumer information that is deidentified or aggregated.</p> <p>However, the CCPA establishes a high bar for claiming data is deidentified or aggregated</p>	<p>Pseudonymous data is considered personal data.</p> <p>Anonymous data is not considered personal data.</p>	<p>The CCPA and GDPR pseudonymization definitions are very similar and both require technical controls to prevent reidentification to qualify.</p>	<p>CCPA</p> <p>Cal. Civ. Code §§ 1798.140(a), (h), (o), (r), and 1798.145(a)(5).</p> <p>Practice Note, California Privacy and Data Security Law: Overview: Personal Information under CCPA (6-597-4106).</p>

	CCPA	GDPR	Comparison	Practical Law Resources and Citations
	Pseudonymous data may qualify as personal information under the CCPA because it remains capable of being associated with a particular consumer or household. However, the statute does not clearly categorize or exclude pseudonymous data as personal information.	While the GDPR does not mention deidentified data, the CCPA definition is similar to GDPR's concept of anonymous data.	The CCPA primarily discusses pseudonymization in the context of using personal information collected from a consumer for other purposes, for research. It does not appear to help businesses generally avoid the CCPA's requirements. At this point, it is unclear how different the position under the GDPR is.	GDPR Article 4(5). Practice Note, Anonymization and Pseudonymization under the GDPR (W-007-4624).
Privacy Notice / Information Right	Businesses must inform consumers about: <ul style="list-style-type: none"> ■ The personal information categories collected. ■ The intended use purposes for each category. Further notice is required to: <ul style="list-style-type: none"> ■ Collect additional personal information categories. ■ Use collected personal information for unrelated purposes. The CCPA requires that businesses provide specific information to consumers and establishes delivery requirements. Third parties must also give consumers explicit notice and an opportunity to opt out before re-selling personal information that the third party acquired from another business.	Data controllers must provide detailed information about its personal data collection and data processing activities. The notice must include specific information depending on whether the data is collected directly from the data subject or a third party.	Similar disclosure requirements, but differences in the specific information required and the delivery methods. The CCPA notice requirements on personal information disclosed or sold to third parties only covers the 12 months preceding the request.	CCPA Cal. Civ. Code §§ 1798.100(a)-(b), 1798.105(b), 1798.110, 1798.115, 1798.120(b), 1798.130, and 1798.135. Practice Note, California Privacy and Data Security Law: Overview: Consumer Rights under the CCPA (6-597-4106) and CCPA Business Obligations (6-597-4106). GDPR Articles 13-14. Practice Note, Data Subject Rights under the GDPR: Personal Data Collected Directly from a Data Subject (W-006-7553) and Personal Data Collected from a Third Party (W-006-7553).
Security	The CCPA does not directly impose data security requirements. However, it does establish a right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk arising from existing California law.	The GDPR requires data controllers and data processors to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	Substantially similar in statutory approach though reasonable security measures may vary to some extent according to an organization's circumstances and regulator interpretation.	CCPA Cal. Civ. Code § 1798.150(a)(1). Practice Note, California Privacy and Data Security Law: Overview: CAG Enforcement and Private Actions under the CCPA (6-597-4106). GDPR Article 24(1). Practice Note, Data security under the GDPR (GDPR and DPA 2018) (UK) (W-013-5138).

	CCPA	GDPR	Comparison	Practical Law Resources and Citations
Opt-Out Right for Personal Information Sales	<p>Businesses must enable and comply with a consumer's request to opt-out of the sale of personal information to third parties, subject to certain defenses.</p> <p>Must include a "Do Not Sell My Personal Information" link in a clear and conspicuous location on a website homepage.</p> <p>Must not request reauthorization to sell a consumer's personal information for at least 12 months after the person opts-out.</p>	<p>The GDPR does not include a specific right to opt-out of personal data sales.</p> <p>However, the GDPR does contain other rights a data subject may use to obtain a similar result in certain circumstances. For example, it does permit data subjects, at any time, to:</p> <ul style="list-style-type: none"> ■ Opt-out of processing data for marketing purposes. ■ Withdraw consent for processing activities. <p>This allows data subjects to opt-out of third-party sales that support marketing purposes or rely on consent for their legal processing basis.</p>	Substantially different.	<p>CCPA</p> <p>Cal. Civ. Code §§ 1798.120 and 1798.135(a)-(b).</p> <p>GDPR</p> <p>Practice Note, Overview of EU General Data Protection Regulation: Processing for Direct Marketing Purposes (W-007-9580) and Lawfulness of Processing (W-007-9580).</p>
Children	<p>The CCPA prohibits selling personal information of a consumer under 16 without consent.</p> <p>Children aged 13 – 16 can directly provide consent. Children under 13 require parental consent.</p> <p>Importantly, protections provided by the federal Children's Online Privacy Protection Act (COPPA) still apply on top of the CCPA's requirements.</p>	<p>The GDPR's default age for consent is 16, although individual member state law may lower the age to no lower than 13. The person with parental responsibility must provide consent for children under the consent age.</p> <p>Children must receive an age appropriate privacy notice.</p> <p>Children's personal data is subject to heightened security requirements.</p>	<p>Substantially different requirements, other than ages involved.</p> <p>The CCPA only requires parental consent for personal data sales, while GDPR's parental consent requirement applies to all processing consent requests.</p>	<p>CCPA</p> <p>Cal. Civ. Code § 1798.120(c)-(d).</p> <p>Practice Note, California Privacy and Data Security Law: Overview: Consumer Rights Under the CCPA (6-597-4106).</p> <p>GDPR</p> <p>Article 8(1).</p> <p>Practice Note, Overview of EU General Data Protection Regulation: Children's consent (W-007-9580).</p>
Right of Disclosure or Access	Consumers have a right to request disclosure of their personal information, and to receive additional details regarding the personal information a business collects and its use purposes, including any third parties with which it shares information.	Data subjects have a right to access their personal data, including receiving a copy and to obtain certain information about the data controller's processing.	<p>Broadly similar rights of disclosure/access.</p> <p>The CCPA's right is only to obtain a written disclosure of the information. The GDPR allows broader access, which is not limited to a written disclosure in a portable format.</p>	<p>CCPA</p> <p>Cal. Civ. Code §§ 1798.100(d), 1798.110, 1798.115.</p> <p>Practice Note, California Privacy and Data Security Law: Overview: Consumer Rights Under the CCPA (6-597-4106).</p> <p>GDPR</p> <p>Article 15.</p> <p>Practice Note, Data Subject Rights Under the GDPR: Personal Data Access Right (W-006-7553).</p>

	CCPA	GDPR	Comparison	Practical Law Resources and Citations
Right of Data Portability	In response to a request for disclosure, a business must provide personal information in a readily useable format to enable a consumer to transmit the information from one entity to another entity without hindrance.	The GDPR includes a new right to data portability to: <ul style="list-style-type: none"> Receive a copy of the personal data in a structured, commonly used and machine-readable format. Transmit the personal data to another data controller (including directly by another data controller where possible). 	Broadly similar rights. The GDPR provides a specific right to request a data controller to transfer their personal data to another data controller.	CCPA Cal. Civ. Code §§ 1798.100(d) and 1798.130(a)(2). Practice Note, California Privacy and Data Security Law: Overview: Consumer Rights Under the CCPA (6-597-4106) GDPR Article 20. Practice Note, Data Subject Rights Under the GDPR: Data portability right (W-006-7553).
Right to Deletion / Erasure (The Right to be Forgotten)	A consumer has the right to deletion of personal information a business has collected, subject to certain exceptions. The business must also instruct its service providers to delete the data.	Data subjects have the right to request erasure of personal data under six circumstances (the right to be forgotten). Data controllers must also take reasonable steps to inform any other data controllers also processing the data.	Similar data deletion rights. The GDPR right only applies if the request meets one of six specific conditions while the CCPA right is broad. However, the CCPA also allows business to refuse the request on much broader grounds than the GDPR. The GDPR's obligation to inform downstream data recipients of the person's deletion request is also broader.	CCPA Cal. Civ. Code § 1798.105. Practice Note, California Privacy and Data Security Law: Overview: Consumer Rights Under the CCPA (6-597-4106) GDPR Article 17. Practice Note, Data Subject Rights under the GDPR: Personal data erasure right ("Right to be forgotten") (W-006-7553).
Right of rectification	None.	The GDPR grants data subjects the right to: <ul style="list-style-type: none"> Correct inaccurate personal data. Complete incomplete personal data. 	Substantially different.	GDPR Article 16. Practice Note, Data Subject Rights under the GDPR: Personal Data Rectification Right (W-006-7553).
Right to Restrict Processing	None, other than the right to opt-out of personal information sales.	Right to restrict processing of personal data, under certain circumstances.	Substantially different.	CCPA Cal. Civ. Code § 1798.120. GDPR Article 18. Practice Note, Data Subject Rights under the GDPR: Data Processing Restriction Right (W-006-7553).
Right to Object to Processing	None, other than the right to opt-out of personal information sales.	Right to object to processing for profiling, direct marketing, and statistical, scientific, or historical research purposes.	Substantially different.	CCPA Cal. Civ. Code § 1798.120. GDPR Article 21. Practice Note, Data Subject Rights under the GDPR: Data Processing Objection Right (W-006-7553).

	CCPA	GDPR	Comparison	Practical Law Resources and Citations
Right to Object to Automated Decision-Making	None.	Data subjects have the right to not be subject to automated decision-making, including profiling, which has legal or other significant effects on the data subject, subject to certain exceptions.	Substantially different.	GDPR Article 22. Practice Note, Data Subject Rights under the GDPR: Automated Decision-Making Objection Right (W-006-7553).
Non-Discrimination	A business must not discriminate against a consumer because they exercised their rights. However, a business may charge differently if that difference reasonably relates to the value provided by the consumer's data. Businesses may also offer financial incentives if they are disclosed in terms or online privacy policy, and require opt-in consent.	It is implicit in the GDPR that organizations cannot discriminate against a data subject that exercises his rights, for example by references prohibiting processing that adversely affects the rights and freedoms of data subjects.	Similar idea, different obligations.	CCPA Cal. Civ. Code § 1798.125.
Responding to Rights Requests	A business must: <ul style="list-style-type: none"> Comply with a verifiable consumer request (as defined in Cal. Civ. Code § 1798.140(y)). Respond within 45 days after receipt, potentially extendable once for another 45 or 90 days on customer notification. Inform the consumer of the reasons for not taking action. Provide the information free of charge, unless the request is manifestly unfounded or excessive. Consumers may only make most information requests twice a year and only for a 12-month look-back. There are no limits on deletion and do not sell requests.	A data controller must: <ul style="list-style-type: none"> Verify the identity of a data subject before responding to a request. Respond to requests without undue delay and at the latest within one month., extendable for up to two more months if necessary after data subject notice. Give reasons if the data controller does not comply with any requests. Requests do not have to be free to data subjects.	Substantially similar.	CCPA Cal. Civ. Code §§ 1798.100(c)-(d), 1798.105(c), 1798.110(b), 1798.115(b), 1798.130(a)(2), (b), 1798.140 (y), and 1798.145(g). GDPR Article 12. Practice Note, Data Subject Rights Under the GDPR: Responding to Data Subject Requests (W-006-7553).
Penalties (Private Rights of Action)	The CCPA establishes a narrow private right of action for certain data breaches involving a sub-set of personal information. However, the CPPA grants companies a 30-day period to cure violations, if possible. Consumers may seek the greater of actual damages or statutory damages ranging from \$100 to \$750 per consumer per incident. Courts may also impose injunctive or declaratory relief.	The GDPR establishes a private right of action for material or non-material damage caused by a data controller or data processors breach of the GDPR.	Substantially different in scope, but violations of either may potentially result in significant economic liability.	CCPA Cal. Civ. Code § 1798.150. Practice Note, California Privacy and Data Security Law: Overview: CAG Enforcement and Private Actions Under the CCPA (6-597-4106). GDPR Article 82. Practice Note, GDPR and DPA 2018: enforcement, sanctions and remedies (UK): Remedies, liability and penalties (W-005-2487).

	CCPA	GDPR	Comparison	Practical Law Resources and Citations
Penalties (Civil Fines)	The California AG may bring actions for civil penalties of \$2,500 per violation, or up to \$7,500 per violation if intentional. However, the CCPA also grants businesses a 30-day cure period for noticed violations.	Administrative fines can reach EUR20 million or 4% of annual global revenue, whichever is highest. EU Member States can impose their own penalties applicable to infringements of the GDPR that are not subject to administrative fines under Article 83, GDPR.	Approach to calculating fines differs, but violations of either may potentially result in significant economic liability.	<p>CCPA</p> <p>Cal. Civ. Code §1798.155.</p> <p>Practice Note, California Privacy and Data Security Law: Overview: CAG Enforcement and Private Actions Under the CCPA (6-597-4106).</p> <p>GDPR</p> <p>Article 83-84.</p> <p>Practice Note, GDPR and DPA 2018: enforcement, sanctions and remedies (UK) (W-005-2487).</p>

CCPA DEFINITIONS

The CCPA has a long list of defined terms (Cal. Civ. Code §1798.140). This box discusses certain defined terms used in this Chart. For the definition of personal information, see Box, Personal Information Categories Under the CCPA.

Controls means:

- Ownership of or the power to vote more than 50 percent of the outstanding shares of any class of voting security of a business.
- Control in any manner over the election of a majority of the directors or of individuals exercising similar functions.
- The power to exercise a controlling influence over the management of a company.

(Cal. Civ. Code § 1798.140(c)(2).)

Common branding means a shared name, service mark, or trademark.

(Cal. Civ. Code § 1798.140(c)(2).)

Service provider means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that:

- Processes information on behalf of a business.
- Receives personal information from a business;
 - for a business purpose only; and
 - under a written contract, which prohibits the service provider from retaining, using, or disclosing the personal information for any purpose other than for performing the services specified in the contract or as otherwise permitted by this title.

(Cal. Civ. Code § 1798.140(v).)

Third party means a person or entity other than the business collecting personal information from consumers under the

CCPA. However, the third party definition excludes personal information recipients who obtain the data:

- Directly from the business.
- For a business purpose.
- Under a written contract that contains specific clauses.

To qualify for the exclusion, the business's written contract with the recipient must:

- Prohibit the recipient from:
 - selling the personal information;
 - retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract; and
 - retaining, using, or disclosing the information outside of the direct business relationship between the recipient and the business.
- Include a certification that the recipient understands the restrictions and will comply with them.

(Cal. Civ. Code § 1798.140(w).)

CCPA EXCEPTIONS TO EXTRATERRITORIAL APPLICATIONS

The CCPA does prevent collections or sales of a California resident's (consumer's) personal information if every aspect of the commercial conduct takes place wholly outside California. To qualify the business must:

- Collect the personal information while the consumer is outside of California.
- Ensure no part of the consumer's personal information sale occurs in California.

- Not sell personal information collected while the consumer was in California.

The CCPA exception does not permit a business to store, including on a device, personal information about the consumer while present in California, and then collect that personal information when the consumer or stored personal information is later outside of California.

(Cal. Civ. Code § 1798.145(a)(6).)

PERSONAL INFORMATION CATEGORIES UNDER THE CCPA

The CCPA defines personal information more broadly than California's other laws. It includes any information that directly or indirectly identifies, describes, relates to, is capable of being associated with, or can reasonably link to a particular consumer or household. The statutory definition includes eleven specific categories that businesses must use when providing their required disclosures. Those categories are:

- **Identifiers**, such as:
 - real name;
 - an alias;
 - postal address;
 - email address;
 - unique personal or online identifier;
 - internet protocol (IP) address;
 - account name;
 - social security number (SSN);
 - driver's license or passport number; or
 - other similar identifiers.
- Personal information categories described in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), which in addition to the identifiers described above, also lists a person's:
 - signature.
 - physical characteristics or description;
 - state identification card number;
 - insurance policy number.
 - education.
 - employment or employment history.
 - bank account number, credit card number, debit card number, or any other financial information.
 - medical information or health insurance information.
- Characteristics of protected classifications under California or federal law, like race, religion, gender, national origin, or

sexual orientation (see State Q&A, Anti-Discrimination Laws: California).

- Commercial information, including records of:
 - personal property;
 - products or services purchased, obtained, or considered; or
 - other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including:
 - browsing history;
 - search history; or
 - information regarding a consumer's interaction with an internet website, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Education information, defined as nonpublic personally identifiable information under the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g and 34 C.F.R. Part 99).
- Inferences drawn from any of these personal information categories to create a profile about a consumer reflecting the consumer's:
 - preferences;
 - characteristics;
 - psychological trends;
 - predispositions;
 - behavior;
 - attitudes;
 - intelligence;
 - abilities; or
 - aptitudes.

INFORMATION EXCLUDED FROM THE CCPA'S PERSONAL INFORMATION DEFINITION

Personal information does not include "publicly available" information. However, the CCPA narrowly defines the "publicly available" term to only mean information lawfully made available from federal, state, or local government records.

The publicly available term does not include:

- Data used for a purpose not compatible with the public recordkeeping purpose that caused the government entity to maintain or make the data available.

- Biometric information collected without the person's knowledge.
- Deidentified or aggregate consumer data.

(Cal. Civ. Code §1798.140(o)(2).)

The CCPA does not apply to:

- Medical information or protected health information governed by California and federal health information privacy laws.
- Clinical trial information subject to the Federal Policy for the Protection of Human Subjects (the Common Rule).
- Personal information regulated by the Fair Credit Reporting Act (FCRA).

(Cal. Civ. Code §1798.145(c)-(d).)

Only one CCPA section providing a private right of action for certain data breaches applies to personal information governed by:

- The Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act.
- Driver's Privacy Protection Act of 1994.

The CCPA's other provisions do not. (Cal. Civ. Code 1798.145(e)-(f).)

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at legalsolutions.com/practical-law. For more information or to schedule training, call **1-800-733-2889** or e-mail referenceattorneys@tr.com.