Crowe

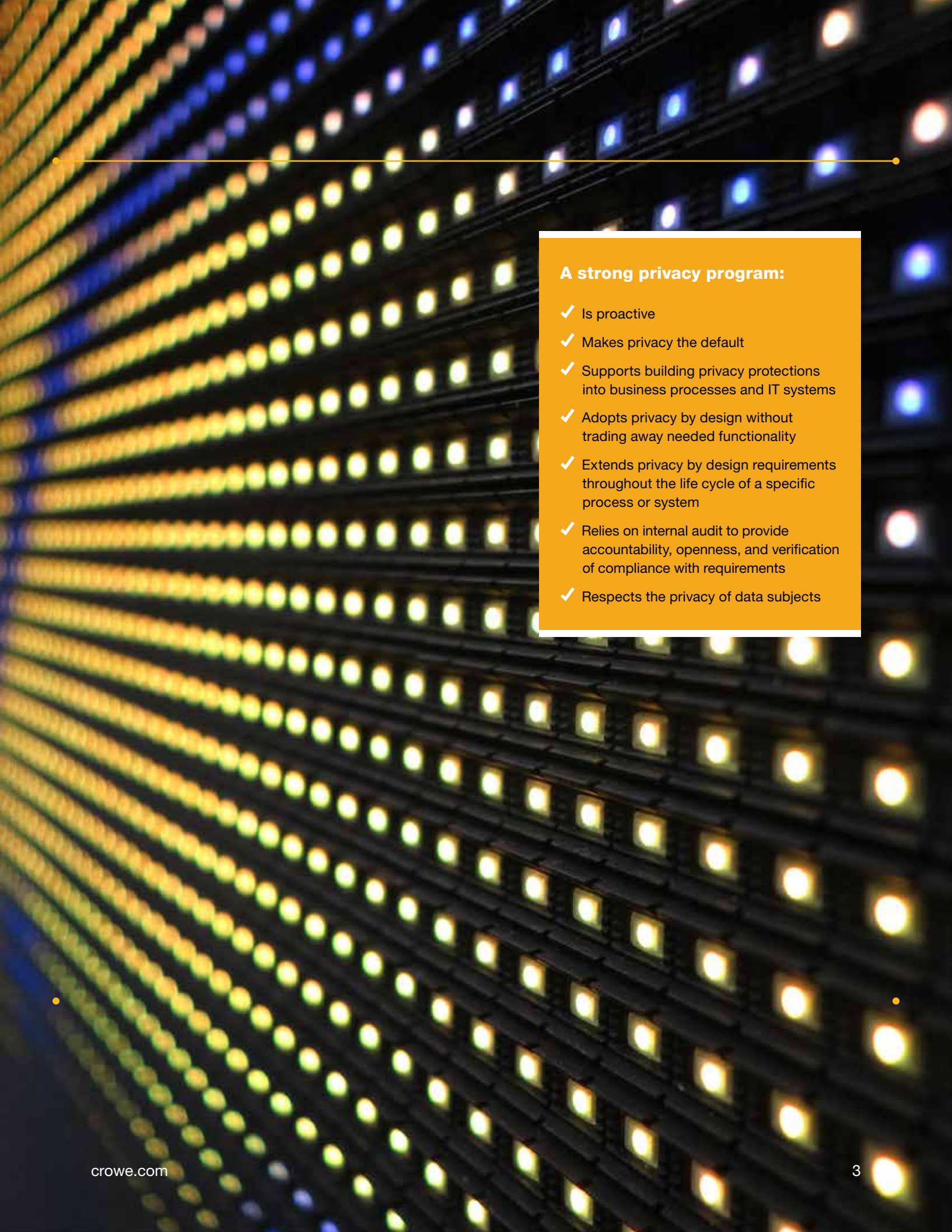
Checklist

Characteristics of a Strong Privacy Program

A checklist by Pamela S. Hrubey, CCEP, CIPP/US, and Lucas Morris, CISSP

For many organizations, building an effective privacy program can be a daunting task. The sheer number of processes involved, the places and ways in which that data is used, and the overwhelming size of the task can easily stymie the development of a solid program. One way for organizations to move forward is to take a risk-based approach by focusing on the highest-risk data and tracking how it is used.

Organizations can develop data privacy programs that form the foundation for positive change in the way personal data is handled while still protecting both data subjects and the organization from the effects of missteps. Strong privacy programs are bolstered by robust internal audit programs. As internal audit enhances existing or builds new data-related audit programs, consider the following checklist of characteristics.



A strong privacy program:

- ✓ Is proactive
- ✓ Makes privacy the default
- ✓ Supports building privacy protections into business processes and IT systems
- ✓ Adopts privacy by design without trading away needed functionality
- ✓ Extends privacy by design requirements throughout the life cycle of a specific process or system
- ✓ Relies on internal audit to provide accountability, openness, and verification of compliance with requirements
- ✓ Respects the privacy of data subjects

A strong privacy program:

✓ Is proactive

- An effective privacy program recognizes the value of considering privacy consistently, the earlier in the process the better.
- With a commitment to privacy at the highest levels of the organization, the program sets and enforces a high standard for privacy-related behaviors.
- Privacy standards might be more far-reaching than local laws require.
- Privacy program leaders make continual improvements to the program based on lessons learned and experiences of employees across the organization.
- Privacy program leaders anticipate the potential for privacy failures and seek ways to prevent those failures from occurring.

✓ Makes privacy the default

- Automatically protecting personal data means that an individual data subject does not have to take a specific action to have their personal data protected.
- The reasons behind the collection, use, retention, and disclosure of personal data are communicated to the specific data subject before or (at a minimum) at the time the personal data is collected, and only personal data related to the specified purpose is collected.
- Collection of personal data is fair and consistent with (or more stringent than) what the law allows.
- Collection of personal data is minimized.
- The use, retention, and disclosure of personal data is limited only to those purposes disclosed to the individual in the privacy notice or to those to which he or she has consented. In some cases, additional retention or use may be required by law or regulation that supersedes other requirements. Finally, personal data should be retained only as long as is necessary to fulfill the stated purposes, after which it is securely destroyed.

✓ Supports building privacy protections into business processes and IT systems

- Privacy protections become an essential component of the base functionality.
- The organization uses accepted fair information practice standards and frameworks that support both internal and external reviews and audits across the enterprise.
- The organization conducts privacy impact and risk assessments and shares the results for purposes of mitigating the identified risks and improving practices over time.
- Any adverse repercussions to privacy protections that result from the use of specific technologies or business practices are minimized. When such adverse effects on privacy protections exist, the organization takes care to routinely monitor performance of the business process or IT systems as an additional precaution.

✓ Adopts privacy by design without trading away needed functionality

- The organization avoids the "we can't do that because of privacy requirements" tradeoff and uses creativity, partnership, and cooperation to accommodate all legitimate business interests and objectives while protecting data subject privacy.
- Embedding privacy into a business process or an IT solution is accomplished in a way that all requirements are optimized.
- The organization avoids presenting privacy requirements as a tradeoff for other requirements.

✓ Extends privacy by design requirements throughout the life cycle of a specific process or system

- The privacy program implements strong security for the duration of the time that personal data is stored, maintained, and destroyed.
- The privacy program establishes a strong partnership with the information security program, and members of the workforce consider privacy and security requirements seamlessly.
- Information security standards support maintaining the confidentiality, integrity, and availability of personal data throughout the entire life cycle of use, from implementation through destruction.

✓ Relies on internal audit to provide accountability, openness, and verification of compliance with requirements

Accountability

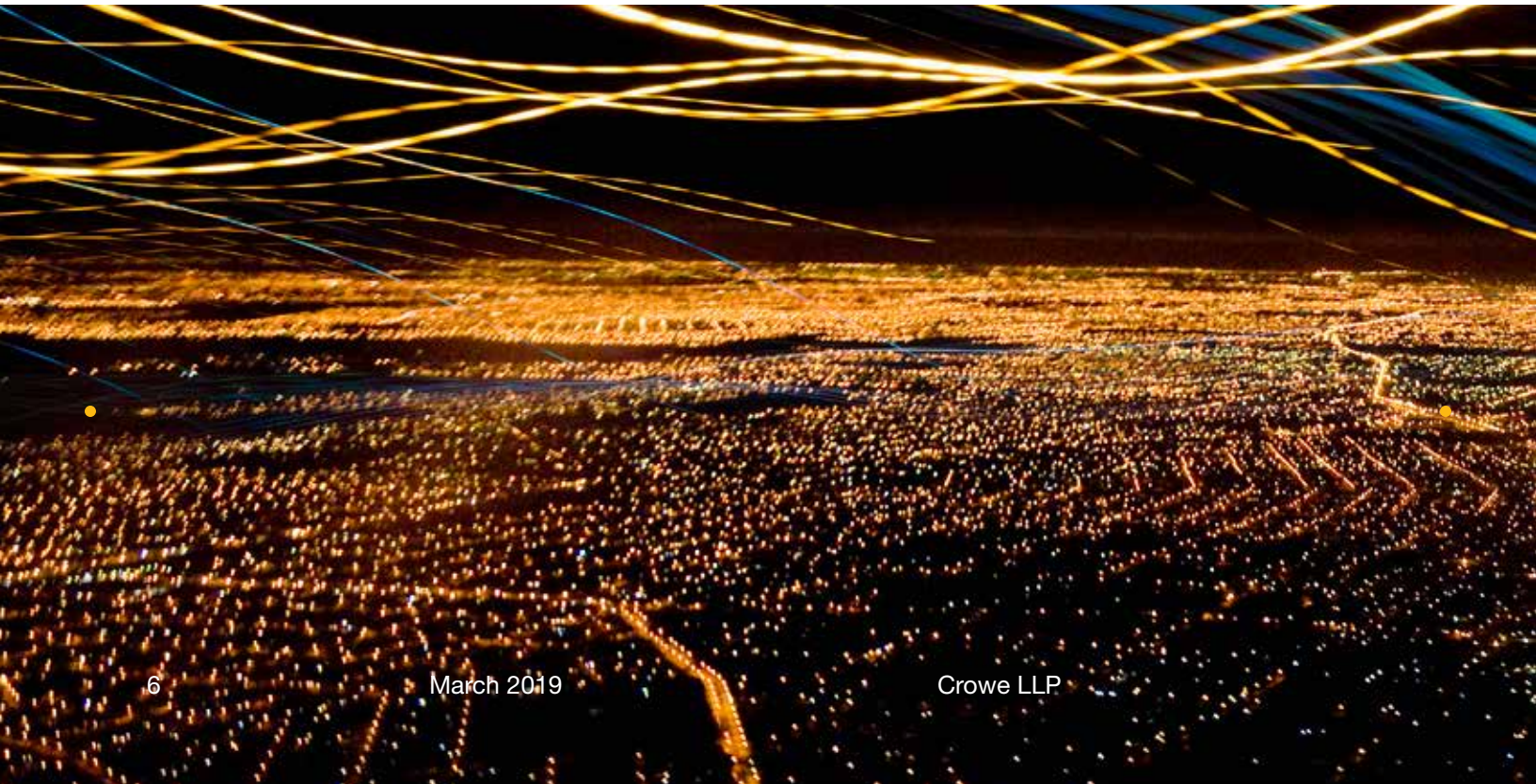
- The organization documents and communicates responsibility for all privacy-related policies and procedures and assigns overall accountability to a specific leader.
- Personal data is only shared with third parties that agree to provide equivalent privacy protection, which is generally secured via contractual agreement. When personal data is shared with third parties, the organization communicates the sharing in privacy notices and consent documentation.

Openness

- Openness and transparency are key to accountability.
- Information about the policies and practices relating to the management of personal data is readily available to those expected to follow them, as well as to those whose personal data is protected by the policies and practices.

Compliance

- The organization provides a mechanism for data subjects to report privacy and data protection-related concerns.
- The organization takes the needed steps to monitor, evaluate, and verify compliance with privacy policies and procedures.



✓ Respects the privacy of data subjects

- All members of the workforce who come into contact with personal data are expected to consider the interests of the data subject and to appropriately protect personal data from inappropriate use, disclosure, or destruction.
- Consent is obtained for the collection, use, or disclosure of personal data, unless collection, use, and disclosure are specifically required by law.
- Personal data is accurate, complete, and up-to-date.
- Individuals have access to their personal data, they can challenge its accuracy and completeness, and they can request that inaccurate data be corrected.
- Individuals can have their personal data deleted (forgotten) when allowed by law.
- Organizations provide data subjects with a readily available mechanism for requesting information or making a complaint about the specific use of the data subject's personal data.

Learn more

Pam Hrubey
Managing Director
+1 317 208 1904
pam.hrubey@crowe.com

Lucas Morris
+1 214 777 5257
lucas.morris@crowe.com

crowe.com

RISK-19001-006F