Managing Privacy and Business after Lockdown

Remote to Reopening Considerations

June 2020

Governments and industries spanning the globe are engaged in the hard and important work of identifying a path forward to reopening the economy post-lockdown. Many companies are contemplating reopening initiatives to ensure a safe and healthy work place and environment for personnel, customers, and guests, including the use of health declarations, thermal screening, contract tracing, and (continued) remote working.

We provide here our high-level recommendations and best practices to consider while assessing and developing your company's reopening initiatives.

Health Declarations

This strategy targets use of surveys or questionnaires focused on identifying high-risk individuals, which can implicate: (1) basic personal information (*e.g.,* name, job title, email address); (2) health information, such as COVID-related symptoms (*e.g.*, fever, shortness of breath, coughing, loss of taste and/or smell); (3) social contact information or self-isolation information; and (4) location information, including recent travel to or from high-risk locations.

- ✓ **Provide supplemental notice** to employees and customers at or before collection.
  - o Notice of collection practices could be in updated privacy notice, back-to-work communications, training, or signage posted in conspicuous areas.
- ✓ Observe **data minimization principles**.
  - o If possible, consider a health declaration strategy that records or logs no personal information.
  - o Only collect personal information essential to protecting the work place and public health.
  - o Retain collected personal information for only as long as necessary for the purpose collected.
- ✓ Observe **disclosure limitations**.
  - o Limit access to discrete personnel (*e.g.*, HR, management, security).
  - o If possible, disclose personal information to third parties only when absolutely necessary or when required by law.
- ✓ **Implement high security protocols** and issue cybersecurity reminders to employees to help protect personal information.

Thermal Screening Recommendations

Temperature screening and thermal imaging are expected to be a large part of reopening plans, which can be employed through a manual, self-administered, or automated process.

- ✓ **Provide a private or quasi-private** area for screening, if possible.
- ✓ Administer **least-intrusive measures** on a **consistent basis**.
- ✓ **Train employees** on the proper administration of screenings.
- ✓ **Develop protocol** for identifying and responding to high-risk individuals.
- ✓ Provide **supplemental notice** to employees, customers, and guests at or before collection.
- ✓ Adhere to rigorous **data minimization principles** – record no data, if possible.
- ✓ Observe **disclosure limitations**:
  - o Limit access to discrete personnel (*e.g.*, HR, management, security).

- If possible, disclose personal information to third parties only when absolutely necessary or when required by law.

- ✓ Implement **security protocols** and issue cybersecurity reminders to employees to help **protect personal information**.

Contract Tracing Recommendations

As lockdown from COVID-19 begin to lift, contact tracing apps intended to help identify and slow the transmission of the virus are being developed and utilized.

- ✓ Contact tracing is **not obligatory**, and mandatory use should be carefully considered.
- ✓ **Third-party apps** have not all been vetted for compliance with applicable laws and may have been rolled out hastily.
- ✓ **Liability and exposure** in the agreements to use third-party apps are extremely important—many contain virtually no protection for the end-user or the company.
- ✓ Take a hard look at **where and when you need the information** to keep your employees and customers safe.
- ✓ Take the **least intrusive** option.

Remote Working Best Practices

Telecommuting and remote working will likely continue as the principal initiative to ensure a safe working environment throughout the pandemic. Carefully consider relevant federal and state rules that require security for, and protection of, personal information.

- ✓ **Basic Security hygiene**: Use encrypted access points (WAP2); require multi-factor authentication; and access limitations.
- ✓ **Technical controls**: Update and test VPNs and network infrastructure devices; deploy patches and upgrades; persistent attack detection and log review; and consider full-disk encryption.
- ✓ **Training and Awareness**: Alert employees to an increase in phishing; and deploy security awareness or refresher security training.
- ✓ **Review & update Incident Response Plans.** Ensure that the incident response team is familiar with the incident response plan and contact information for key personnel is up-to-date.

Data Privacy Key Considerations

Though strategies designed to ensure a safe work place may vary based on company and industry, key privacy and security considerations should—at a minimum—include:

- ✓ Observing transparency about the purpose for collection, the data elements collected, the retention period, and disclosure practices.
- ✓ Ensuring privacy policies are updated or supplemented.
- ✓ Collecting personal information only for public health and safety purposes, and only personal information necessary to maintain a safe environment.
- ✓ Providing appropriate safeguards to secure the data**.**
- ✓ Restricting access to personal information or health status without consent, and minimizing the data shared.
- ✓ Deleting personal information as soon as it is no longer needed.
- ✓ Employing anonymization or pseudonymization techniques, if possible.
- ✓ Observing, respecting, and responding to data subject rights, where applicable.

For additional guidance, please contact a member of the Privacy and Data Security Team below.

Matthew R. Baker
Partner
T: +1.415.291.6213
matthew.baker@bakerbotts.com

Neil Coulson
Partner
T: +44.20.7726.3478
neil.coulson@bakerbotts.com

Maureen Ohlhausen
Partner
T: +1.202.639.7726
maureen.ohlhausen@bakerbotts.com

Cynthia Cole
Special Counsel
T: +1.650.739.7575
cynthia.cole@bakerbotts.com