Gesamtbetriebsvereinbarung

über die Einsicht in
personenbezogene und personenbeziehbare Datenbestände

Präambel

Prävention und Abwehr von äußeren und inneren Gefahren gehören zu den Kernaufgaben der für Security und Compliance verantwortlichen Stellen des Unternehmens. Maßnahmen der Gefahrenabwehr betreffen in verstärktem Maße insbesondere die Bereiche der EDV und der IT. Dabei sind das berechtigte Interesse am Schutz des Unternehmens ebenso wie die berechtigten Interessen der Beschäftigten und der Vertraulichkeit der Daten in Einklang zu bringen.

Im Bayer-Konzern werden diesbezügliche Einsichtnahmen insbesondere durch die

- Direktive 2005 „Nutzung und Überprüfung dienstlicher E-Mail-Systeme im Bayer-Konzern",
- Direktive 2008 „Authorizations in Business Applications"
- Direktive 2029 „Bearbeitung von Compliance-Vorfällen"
- Direktive 1396 „Datenschutz"

beschrieben und geregelt. Darin wird regelmäßig auch auf die Beteiligung der Mitbestimmungsgremien verwiesen. Diese Beteiligung des Betriebsrates soll durch die vorliegende Gesamtbetriebsvereinbarung näher konkretisiert werden.

I. Geltungsbereich

Diese Gesamtbetriebsvereinbarung wird abgeschlossen für alle Beschäftigten der Bayer AG sowie kraft Vollmacht der mit der Bayer AG verbundenen Konzernunternehmen Bayer CropScience AG, Bayer MaterialScience AG, Bayer HealthCare AG, Bayer Pharma AG, Bayer Animal Health GmbH, Bayer Business Services GmbH, Bayer Technology Services GmbH, Bayer Direct Services GmbH, Bayer Intellectual Property, der Bayer MaterialScience Energiegesellschaft Brunsbüttel und Pallas AG (alle Gesellschaften nachstehend „GESELLSCHAFTEN" genannt).

Sie gilt nicht für Leitende Angestellte i.S.d. § 5 Abs. 3 BetrVG der GESELLSCHAFTEN.

II. Grundsätze

- Untersuchungen, bei denen insbesondere das Internetverhalten, das E-Mail-Postfach oder der Computerinhalt eines einzelnen Beschäftigten ausgewertet werden soll (s. Ziff. IV bis IX dieser Gesamtbetriebsvereinbarung), sind besonders sensibel. Hierbei können Persönlichkeitsrechte oder die Privatsphäre von Beschäftigten betroffen sein, so dass derartige Untersuchungen unter Beachtung der Schutz- und Informationsrechte der Beschäftigten durchzuführen sind. Dabei sind Untersuchungen, die sich auf einen oder mehrere Beschäftigte bezie-

hen, grundsätzlich objektiv und unter Wahrung der berechtigten Interessen der Betroffenen sowie der Wahrung der Verhältnismäßigkeit zu führen.

- Vertretungsregelung
  Die Vertraulichkeit der Daten ist auch bei einem notwendigen betrieblichen Zugriff zu gewährleisten, unter anderem durch die Nutzung verbindlicher Vertretungsregelungen. Für längerfristige Abwesenheiten und Personalwechsel sind transparente und eindeutige Verfahrensweisen von den Führungsverantwortlichen mit der zuständigen IT-Administration festzulegen und allgemein bekannt zu machen. Das Setzen oder Löschen von Statusinformationen (Abwesenheitsagent bzw. Lync-Notiz) kann auf schriftlichen Antrag des Vorgesetzten umgesetzt werden. Ist dennoch ein dringender und betrieblich notwendiger Zugriff auf die Daten eines abwesenden Mitarbeiters notwendig, so kann nach schriftlichem Antrag des Vorgesetzten ein Lesezugriff erteilt werden, wobei der Betroffene (dies gilt nicht bei bereits ausgeschiedenen Beschäftigten) informiert wird, bspw. über eine entsprechende eMail. In allen Fällen ist der zuständige Betriebsrat im Vorfeld einzubeziehen.

- Sonderregelungen für besondere Personengruppen

  Personengruppen, die einer besonderen Schweigepflicht unterliegen, zum Beispiel Betriebsrat, Jugend & Auszubildenden- , Schwerbehindertenvertretung, ärztlicher Dienst und Sozialberatung, sind vom Anwendungsbereich dieser Betriebsvereinbarung ausgeschlossen. In Fällen hinreichenden Verdachts eines strafrechtlich relevanten Fehlverhaltens durch Mitarbeiter vorgenannter Personengruppen ist die Dateneinsichtnahme unter Berücksichtigung besonderer rechtlicher Voraussetzungen möglich, die dem Gesamtbetriebsratsvorsitzenden bzw. dem stellvertretenden Gesamtbetriebsratsvorsitzenden im Vorfeld mitgeteilt werden.

- Auftraggebende Stelle
  In der Regel werden interne Untersuchungen durch Geschäftsleitung, Compliance Organisation, Corporate Auditing, Corporate Security, Rechtsabteilung oder HR eingeleitet und geführt.

- Untersuchende Stelle
  Die Einsichtnahme in personenbezogene Daten erfolgt durch Corporate Auditing, Corporate Security, die Securityverantwortlichen der Gesellschaften oder lokale Site Security. Ziel der Einsichtnahme und die weiteren Schritte sind gemäß dieser GBV zu dokumentieren.

- Ist unklar, welcher Standort betroffen ist oder sind mehrere Standorte betroffen, werden der Gesamtbetriebsrat und der lokale Betriebsrat informiert. Soweit in dieser Gesamtbetriebsvereinbarung von „Betriebsrat" die Rede ist (und nicht anderweitig definiert), ist damit der/die Vorsitzende des jeweiligen lokal zuständigen Betriebsrats gemeint. Ist der Vorsitzende nicht erreichbar, tritt an dessen Stelle sein/e Stellvertreter/in. Gleiches gilt in analoger Weise für den Gesamtbetriebsrat, soweit dieser einzubeziehen ist.

- Die auftraggebende Stelle entscheidet über Art und Weise, wie die Untersuchungen – unter Berücksichtigung dieser Gesamtbetriebsvereinbarung – durchgeführt werden. Dies gilt insbesondere zur Identifizierung eines möglichen Verursachers im Anfangsstadium der Untersuchungen unter Zugriff auf die dazu notwendigen Verbindungsdaten. Der Zugriff auf personenbezogene Daten erfolgt durch die untersuchende Stelle, die die weiteren Schritte mit dem Betriebsrat in der im Folgenden beschriebenen Weise abstimmt. Eine unternehmensseitig veranlasste Datensicherung ohne Datensichtung bedarf nicht der Zustimmung des Betriebsrats.

III. Ablaufbeschreibung der Kontrolle des Internetverhaltens

1) Auswertungen des über die IP-Adresse des PC-Anschlusses laufenden Internet-Datenstroms einzelner Beschäftigter sind zulässig, wenn der Verdacht auf ein Fehlverhalten des Beschäftigten oder auf eine unzulässige Nutzung besteht. Dies ist insbesondere der Fall bei dem Verdacht, dass Handlungen begangen wurden, die eine Vertragsverletzung zu Lasten der GESELLSCHAFT beinhalten, straf- oder bußgeldrechtliche Folgen nach sich ziehen und/oder zu Schadensersatzforderungen einer GESELLSCHAFT oder Dritter gegenüber einer Gesellschaft des Bayer-Konzerns führen können.

2) Die Kontrolle der Internet-Nutzung darf nur durch die auftraggebende Stelle veranlasst werden. Hierbei beantragt die auftraggebende Stelle, unter ausreichender Schilderung des Sachverhalts und der Verdachtsmomente, die Kontrolle der Internet-Nutzung beim Konzern-Datenschutzbeauftragten und holt dessen Zustimmung ein. Die Entscheidung ist mit dem zuständigen Betriebsrat abzustimmen.

3) Nach Genehmigung informiert der Konzern-Datenschutzbeauftragte die auftraggebende Stelle und leitet den Antrag zur Durchführung an die Geschäftsführung der Bayer Business Services GmbH (BBS) weiter. Diese veranlasst die Überprüfung der IP-Adresse des entsprechenden PC-Anschlusses.

   Ausschließlich von der Geschäftsführung der BBS autorisierte Administratoren sind befugt, der untersuchenden Stelle den Inhalt der Auswertung zur Verfügung zu stellen.

   Bei allen nicht von der BBS betriebenen PC-Anschlüssen klärt der Vorgesetzte der Administratoren, wer der Ansprechpartner für den jeweiligen PC-Anschluss ist und sorgt dafür, dass die Administratoren entweder per Fernverbindung oder vor Ort auf die Datensicherung der entsprechenden IP-Adresse zugreifen können. Dabei werden dem externen Betreiber lediglich die für die Bereitstellung der Analyse notwendigen Daten übergeben (Zeitraum, IP-Adressen und UserID).

   Die Durchführung der Auswertung erfolgt unter Hinzuziehung des Betriebsrats.

4) Auf Basis der Datensichtungsergebnisse entscheidet die untersuchende Stelle, nach Beratung mit dem hinzugezogenen Betriebsrat und HR, über das weitere Vorgehen und eine etwaig notwendige Anhörung des / der Beschäftigten zum Sachverhalt.

5) Die Untersuchungsergebnisse werden in einem schriftlichen Bericht festgehalten. Die untersuchende Stelle informiert den Konzern-Datenschutzbeauftragten und den Betriebsrat spätestens zum Abschluss der Untersuchung über das Ergebnis. Hat sich der Anfangsverdacht durch die Untersuchung bestätigt, wird die zuständige HR Funktion einbezogen und erhält den Untersuchungsbericht.

6) Die für die Analyse bereit gestellten Daten sind nach Abschluss der Untersuchung zu löschen, soweit sie nicht als Beweismaterial für ein sich anschließendes bzw. zu erwartendes internes oder externes Verfahren erforderlich sind.

IV. Ablaufbeschreibung der Kontrolle des E-Mail-Postfachs

1) Auswertungen des E-Mail-Postfachs einzelner Beschäftigter sind zulässig, wenn der Verdacht auf ein Fehlverhalten des Beschäftigten oder auf eine unzulässige Nutzung besteht. Dies ist insbesondere der Fall bei dem Verdacht, dass Handlungen begangen wurden, die eine Vertragsverletzung zu Lasten der GESELLSCHAFT beinhalten, straf- oder bußgeldrechtliche Folgen nach sich ziehen und/oder zu Schadensersatzforderungen einer GESELLSCHAFT oder Dritter gegenüber einer Gesellschaft des Bayer-Konzerns führen können.

2) Die Kontrolle des E-Mail-Postfachs darf nur durch die auftraggebende Stelle veranlasst werden. Hierbei beantragt die auftraggebende Stelle unter ausreichender Schilderung des Sachverhalts und der Verdachtsmomente die Kontrolle des E-Mail-Postfachs beim Konzern-Datenschutzbeauftragten und holt dessen Zustimmung ein. Die Entscheidung ist mit dem zuständigen Betriebsrat abzustimmen. Eine Zustimmungsverweigerung ist durch den Betriebsrat sachgerecht und zeitnah zu begründen.

3) Nach Genehmigung informiert der Konzern-Datenschutzbeauftragte die auftraggebende Stelle und leitet den Antrag zur Durchführung an die Geschäftsführung der Bayer Business Services GmbH (BBS) weiter. Diese veranlasst die Bereitstellung der betreffenden E-Mails und ggf. der zugehörigen Verbindungsdaten.

   Ausschließlich von der Geschäftsführung der BBS autorisierte Administratoren sind befugt, der untersuchenden Stelle den Inhalt der Auswertung zur Verfügung zu stellen. Die Durchführung der Auswertung erfolgt unter Hinzuziehung des Betriebsrates. Der Betriebsrat reagiert unverzüglich.

4) Auf Basis der Datensichtungsergebnisse entscheidet die untersuchende Stelle, nach Beratung mit dem hinzugezogenen Betriebsrat und HR, über das weitere Vorgehen und eine etwaig notwendige Anhörung des / der Beschäftigten zum Sachverhalt.

5) Die Untersuchungsergebnisse werden in einem schriftlichen Bericht festgehalten. Die untersuchende Stelle informiert den Konzern-Datenschutzbeauftragten und den Betriebsrat spätestens zum Abschluss der Untersuchung über das Ergebnis. Hat sich der Anfangsverdacht durch die Untersuchung bestätigt, wird die zuständige HR Funktion einbezogen und erhält den Untersuchungsbericht.

6) Die für die Analyse bereit gestellten Daten sind nach Abschluss der Untersuchung zu löschen, soweit sie nicht als Beweismaterial für ein sich anschließendes bzw. zu erwartendes Verfahren erforderlich sind.

V. Ablaufbeschreibung der Kontrolle persönlich zugeordneter Speicherbereiche

1) Auswertungen persönlich zugeordneter Serverlaufwerke, anderer vergleichbarer Speicherbereiche oder externer Speichermedien einzelner Beschäftigter sind zulässig, wenn der Verdacht auf ein Fehlverhalten des Beschäftigten oder auf eine unzulässige Nutzung besteht. Dies ist insbesondere der Fall bei dem Verdacht, dass Handlungen begangen wurden, die eine Vertragsverletzung zu Lasten der GESELLSCHAFT beinhalten, straf- oder bußgeldrechtliche Folgen nach sich ziehen und/oder zu Schadensersatzforderungen einer GESELLSCHAFT oder Dritter gegenüber einer Gesellschaft des Bayer-Konzerns führen können.

2) Die Kontrolle persönlich zugeordneter Speicherbereiche darf nur durch die auftraggebende Stelle veranlasst werden. Hierbei beantragt die auftraggebende Stelle unter ausreichender Schilderung des Sachverhalts und der Verdachtsmomente die Kontrolle des betroffenen Server-Laufwerks oder Speicherbereichs bei dem Konzern-Datenschutzbeauftragten und holt dessen Zustimmung ein. Die Entscheidung ist mit dem zuständigen Betriebsrat mit der Absicht einer einvernehmlichen Lösung zu beraten. Nach Genehmigung informiert der Konzern-Datenschutzbeauftragte die auftraggebende Stelle und leitet den Antrag zur Durchführung an die Geschäftsführung der Bayer Business Services GmbH (BBS) weiter. Diese veranlasst eine Sicherung der notwendigen Daten.

   Ausschließlich von der Geschäftsführung der BBS autorisierte Administratoren sind befugt, der untersuchenden Stelle die Inhalte der Auswertung zur Verfügung zu stellen. Die Durchführung der Auswertung erfolgt unter Hinzuziehung des Betriebsrates, dies gilt auch für Da-

ten, die auf mobiler Hardware (bspw. CD´s, USB-Stick, externe Festplatte, Laptop oder PC) gespeichert sind. Kann nicht sichergestellt werden, dass es dadurch zu keiner unnötigen Verzögerung des Verfahrens kommt, ist die untersuchende Stelle allein durchführungsberechtigt.

3) Auf Basis der Datensichtungsergebnisse entscheidet die untersuchende Stelle nach Beratung mit dem hinzugezogenen Betriebsrat und HR über das weitere Vorgehen und eine etwaig notwendige Anhörung des / der Beschäftigten zum Sachverhalt.

4) Die Untersuchungsergebnisse werden in einem schriftlichen Bericht festgehalten. Die untersuchende Stelle informiert den Konzern-Datenschutzbeauftragten und den Betriebsrat spätestens zum Abschluss der Untersuchung über das Ergebnis. Hat sich der Anfangsverdacht durch die Untersuchung bestätigt, wird die zuständige HR Funktion einbezogen und erhält den Untersuchungsbericht.

5) Die für die Analyse bereit gestellten Daten sind nach Abschluss der Untersuchung zu löschen, soweit sie nicht als Beweismaterial für ein sich anschließendes bzw. zu erwartendes Verfahren erforderlich sind.

VI. Litigation

1) Neben der in Ziff. IV und V beschriebenen Verfahrensweise kann die Rechtsabteilung veranlassen, dass elektronische Postkörbe und persönlich zugeordnete Serverlaufwerke und Speicherbereiche gesichert werden, soweit dies im Rahmen von anhängigen oder möglichen Rechtsfällen bzw. behördlichen Ermittlungen im In- und Ausland – etwa nach US-amerikanischem Recht – zur Verteidigung oder Durchsetzung der Interessen einer Bayer-Gesellschaft erforderlich und rechtlich zulässig ist, und nach den für das entsprechende Verfahren relevanten elektronischen Dokumenten durchsucht werden. Dies gilt auch für Postkörbe nicht mehr aktiver Mitarbeiter, von denen die Rechtsabteilung eine Sicherungskopie erhalten hat. Die relevanten Dokumente können den Prozessparteien im Rahmen des gerichtlichen oder behördlichen Verfahrens offen gelegt werden. Hierüber werden der zuständige Datenschutzbeauftragte und der Gesamtbetriebsratsrat vorab informiert.

2) Die Rechtsabteilung bewahrt gesicherte Postkörbe auf, solange dies mit Blick auf anhängige oder mögliche Rechtsfälle bzw. behördliche Ermittlungen im In- und Ausland erforderlich ist. Hierauf wird in den Anordnungen zur Aufbewahrung von Dokumenten und den Erinnerungen an die Fortgeltung der Aufbewahrungspflicht hingewiesen.

VII. Externe Ermittlungen / Ansprüche gegen einzelne Beschäftigte

1) Die Herausgabe von personenbezogenen Daten an Dritte bedingt das Vorliegen eines behördlichen Verfahrens.

2) Sofern eine Behörde im Rahmen von Vor- oder Hauptermittlungen eines Straf- oder Ordnungswidrigkeitenverfahrens von der GESELLSCHAFT IT-relevante Informationen (z. B. über die IP-Adresse des PC-Anschlusses eines Mitarbeiters, Zugriff auf das E-Mail-Postfach, Auswertung des Internetverhaltens, etc.) verlangt, die einen oder mehrere Beschäftigte belasten können, ist der Vorgang sofort der Rechtsabteilung zur Prüfung vorzulegen. Die Rechtsabteilung bindet ggf. den Konzern-Datenschutzbeauftragten ein und entscheidet über das weitere Vorgehen. Der Betriebsrat wird zum frühestmöglichen Zeitpunkt informiert.

3) Die Ermittlungsautonomie der Behörden bleibt unberührt. Im Hinblick auf die Verfahrensdurchführung, das Analyseergebnis sowie die Information des Beschäftigten hierüber, kann es aufgrund der Verpflichtung, Informationen an die Behörde weiter zu geben (insbesondere

bei Durchsuchungen und Beschlagnahmen), zu Abweichungen gegenüber dem in dieser Gesamtbetriebsvereinbarung geregelten Verfahren kommen.

4) Gleiches gilt entsprechend, wenn privatrechtliche Ansprüche geltend gemacht werden, die zunächst gegen eine GESELLSCHAFT gerichtet werden (z. B. Ansprüche wegen Urheberrechtsverletzungen, die vom Beschäftigten mittels des dienstlichen Computers begangen werden).

VIII. Schlussbestimmungen

1) Rechte und Pflichten der Beteiligten, die sich aus anderen Gesamtbetriebsvereinbarungen ergeben, bleiben von dieser Gesamtbetriebsvereinbarung unberührt.

2) Diese Gesamtbetriebsvereinbarung tritt mit Unterzeichnung in Kraft und gilt zunächst befristet bis zum 30.06.2014. Die Befristung dient der Erprobung. Corporate Auditing, HR und Gesamtbetriebsrat werden rechtzeitig vor Fristablauf die Gespräche mit der Absicht aufnehmen, die Vereinbarung auf unbestimmte Zeit fortzusetzen.

Leverkusen, den 24.01.2013

.....	.....
Bayer AG	Gesamtbetriebsrat Bayer